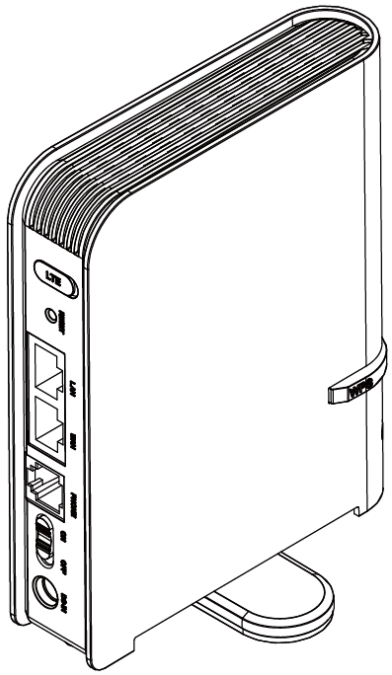
User Manual

BandLuxe

R529

LTE/EVDO Rev. A

VOIP Router



P/N:64013100011 Rev.A

Table of Contents

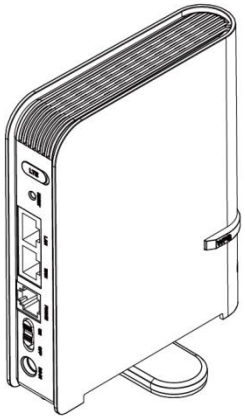
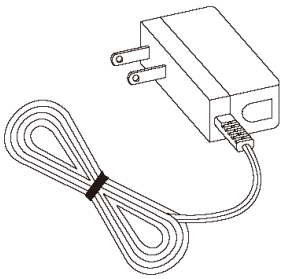
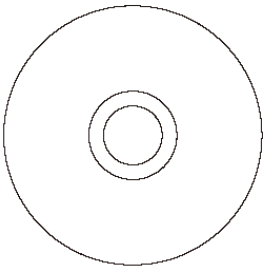
Table of Contents 1
Package Contents 3
Package Contents 3
Features 3
Hardware Overview 4
Installation 6
Basic Functions 8
Wizard Setup 14
Internet Setup 16
Basic Setting 16
DDNS 19
Host 20
Time 21
Router Setup 22
Router password and Network setting 22
Advanced Routing 24
WiFi Setup 26
Basic WiFi Network 26
WPS 32
4G LTE Setup 33
PIN Verification 33
PIN Management 34
SIM Management 35
Preferred Network 36
Security Setup 37
Firewall 37
Internet Access Policy 39
Single Port Forward 42
Port Range Forward 43
Port Range Trigger 44

QoS 45
Status 48
4G LTE & Internet 48
Router 50
Telephony 52
VOIP 52
Appendix A: FAQ 53
Appendix B: Specification 59
Appendix C: Important Safety Information and Glossary ..62
Europe – EU Declaration of Conformity 62
Federal Communication Commission Interference Statement 63
Glossary 65

Package Contents

Thank you for your purchase of this LTE/EVDO VOIP Router. This product is designed to access the Internet via 4G technology and share the bandwidth through a Wi-Fi network. It is easy to configure and operate even for non-technical users. This manual contains instructions for installing and configuring the product. Read the manual carefully before you use the product, so that you can fully exploit the product functions.

Package Contents

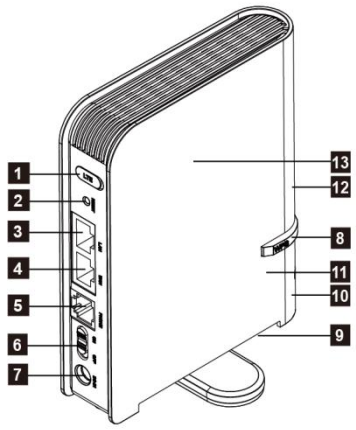
		
LTE/ EVDO VOIP Router	*Power Adaptor*	*User Manual CD*

Features

- LTE/EVDO VOIP Router
- Wi-Fi Protected Setup (WPS) Support
- Supports VOIP over RJ11 (Analog Phone)
- Uplink up to 50 Mbps , Downlink up to 100Mbps
- Supports Wi-Fi 802.11 b/g/n

- Operating Frequency Bands
  - LTE: Band 2/4/12/17/25
  - EVDO: BC 0/1/15
- Supports WAN/LAN Ethernet Port
- Dual embedded cellular antenna (for diversity)

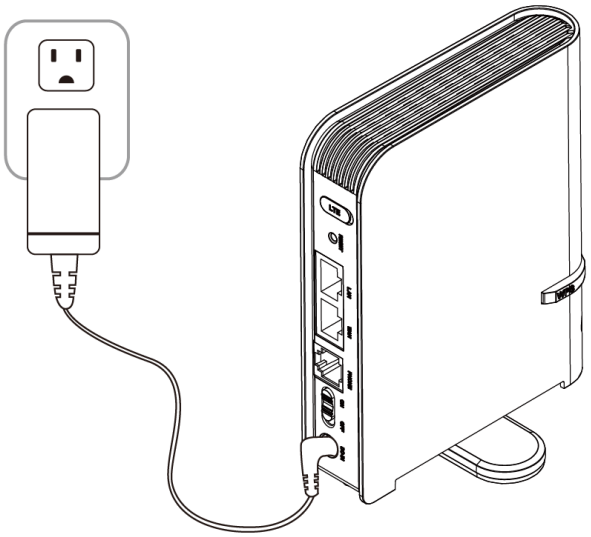
Hardware Overview



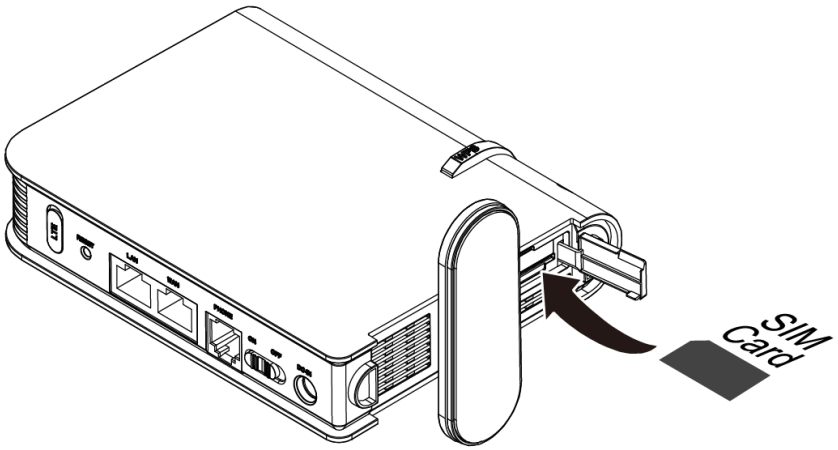
1	**4G External Antenna Port**	To connect the main 4G External Antenna if needed.
2	**Reset Button**	To reset the Router, press the reset button briefly. To restore the Router's factory settings, press the reset button for longer than 5 sec.
3	**LAN Port**	Connect Ethernet devices such as computers, switches, and hubs.
4	**WAN Port**	Connect a DSL or Cable modem.
5	**RJ11 Port**	Connect an analog phone.
6	**Power Switch**	To switch on/off the router.
7	**Power Receptor**	Receptor for the Power Adaptor.
8	**WPS Button**	To enable WPS, press the WPS button for longer than 5 sec. To disable Screen Saver, press the WPS button briefly.

9	**SIM Slot**	Insert SIM/USIM. Push-push type.
10	**4G External Antenna Port**	To connect the secondary 4G External Antenna if needed.
11	**Power LED**	Solid light indicates that the power supply is connected properly.
12	**WiFi External Antenna Port**	To connect to a WiFi External Antenna if needed.
13	**Liquid Crystal Display**	Indicates the status of router. Please reference the details of main screen.

Installation



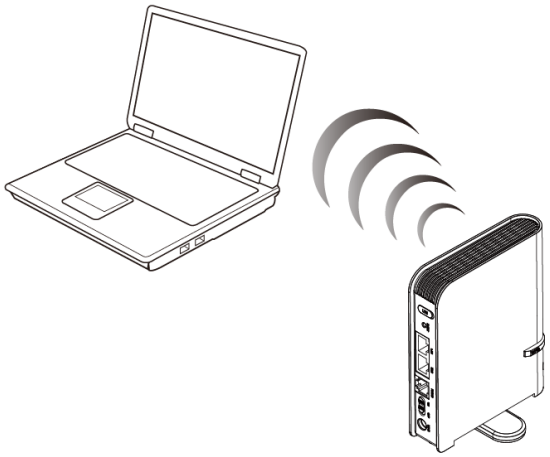
1. Connect the power adaptor to the Router and connect it to an outlet.



2. Insert your SIM card into the slot on the Router, making sure the SIM card orientation matches the SIM card slot, as shown in the picture.

3. Slide the power switch to ON.

4. One of the following two methods can be chosen to link your Router with a PC.

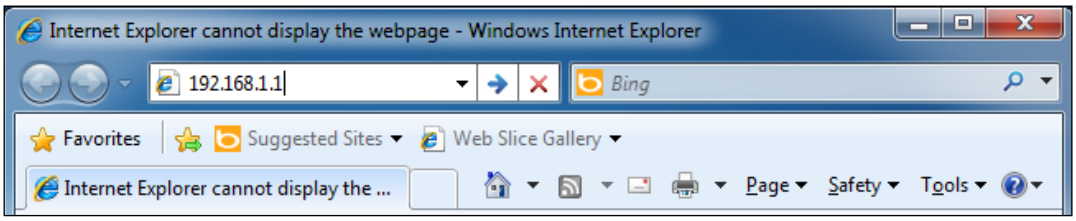


A. To link the Router with your PC via Wi-Fi, in Microsoft Windows, go to *Control Panel* > ***Network Connections***, right-click on **Wireless Network Connection**, and choose **View Available Wireless Networks**. Choose the SSID of the Router wireless network, input the WiFi password if needed and click **Connect**.

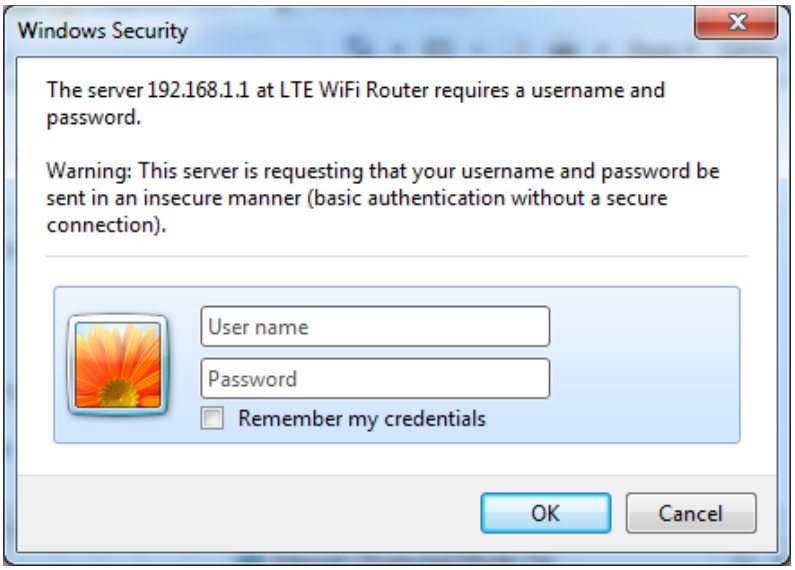
B. To link the Router with your PC via Ethernet cable, connect one end of the cable to the LAN port on the Router, and the other end of the cable to the Ethernet port on your computer.

Note: If you choose to access the Internet via Ethernet, connect one end of the cable to the WAN port of Router, and the other end to your xDSL/Cable Modem.

The Router uses a web-based configuration utility. To access the configuration utility, open a browser (for example Internet Explorer) and enter the IP address (**http://192.168.1.1**) or the URL (**http://R500.ROUTER**) for the Router in your browser's address bar.



Enter the Router User name and Password.


Windows Security
The server 192.168.1.1 at LTE WiFi Router requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name
Password
Remember my credentials
OK
Cancel

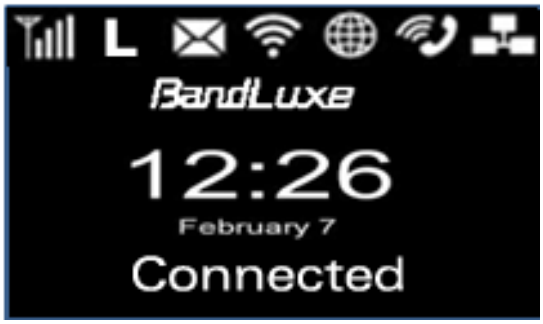
Basic Functions

Powering On and Off

To power the router on, slide the power switch located on the side of the chassis to the ON position. When the router is powered on, the screen displays a series of power-on animations for several seconds.

Main Screen

The Main Screen is the default display screen and provides a quick glance at the status of the device. The screen enters screen saver mode after 60 seconds of inactivity.

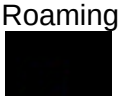
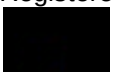


	Signal Strength
	Type of Radio Access Technology
	Short Messaging Service (SMS)
	WLAN On/Off
	Radio Access Roaming On/Off
	VoIP status
	Ethernet status
	Subscriber's Network Operator
	Date & Clock
	Connection Status

Status Indicators

The top of the screen may display the following icons, depending on the status of the device.

Signal Strength	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Radio Access Network	LTE	CDMA/EVDO				
SMS	New SMS	No SMS				

WiFi	WiFi On	WiFi Off				
Roaming	Roaming	Not Roaming 				
VoIP Status	Registered	Not Registered 				
Ethernet	Connected	No Connection				

The Signal Strength icon indicates the relative strength of the radio signal from the nearest base station.

The Radio Access Network icon indicates the subscriber's network mobile technology. It may vary from user to user and from region to region.

The SMS icon indicates whether the mobile subscriber has received new messages from the Short Messaging Service.

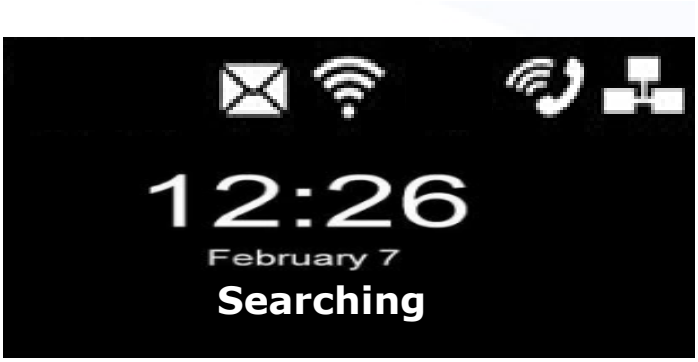
The WiFi icon indicates whether the WiFi feature is enabled or disabled.

The Roaming icon indicates whether the SIM is in roaming status or not.

The VoIP status icon indicates VOIP settings are able to register to a VOIP server.

The Ethernet icon indicates if a PC is connected to the LAN port or if a router is connected to the WAN port.

Other Device Information



Upon inserting a SIM card, the router begins to search for a signal from the network provider. If the signals from the network provider can not be reached, **No Service** is displayed. If the router is connected to radio access network, then the network provider name, type of radio access technology and signal strength are displayed.

If the router can not read the inserted SIM card, **Read SIM Fail** is displayed on the screen. Try removing and re-inserting the SIM card. If the problem persists, contact your network service provider to replace the SIM card.

If the supported SIM card is locked to a specific ISP, **Invalid SIM** is displayed when the Mobile Country Code (MCC) or Mobile Network Code (MNC) does not match

When a VOIP Call is initiated or received, the screen updates to provide information such as Incoming or Outgoing call indication, phone number, and call connection indicator (once the current call is connected).

Enabling WPS

Wi-Fi Protected Setup (WPS) is a standard designed for easy setup and

automatic configuration of secure Wi-Fi networks between two WPS supported devices. If your wireless adapter supports WPS, the WPS feature can be a user-friendly and simple process to get your Wi-Fi network up and running.

1. Enable WiFi.

2. Press and hold the WPS button for at least 5 seconds. **WPS connecting** is displayed.

3. Confirm the WPS option on your wireless adapter trying to connect to the device. **New device connected** is displayed. If you do not confirm the WPS connection within 2 minutes, **No Device found** is displayed and you must begin the process again.

When WPS is enabled, the screen automatically reverts to the Main Screen after a period of inactivity when WPS is enabled.

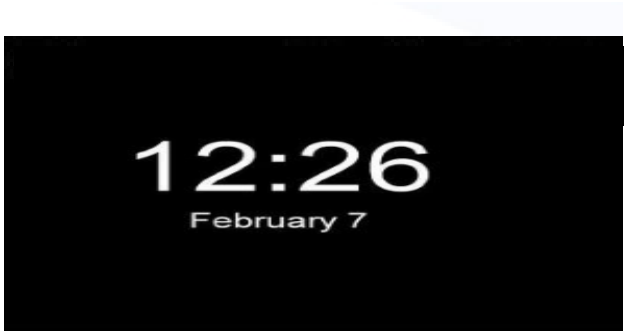
Notifications

If the firmware version on the device is being updated via the Web interface, the screen informs the user of the process.

If the user has enabled the PIN security protection on the SIM card, the screen directs the user to access **4G LTE > PIN Verification** via the web interface before proceeding to use the Internet connectivity features of

the device.

Screen Saver Mode

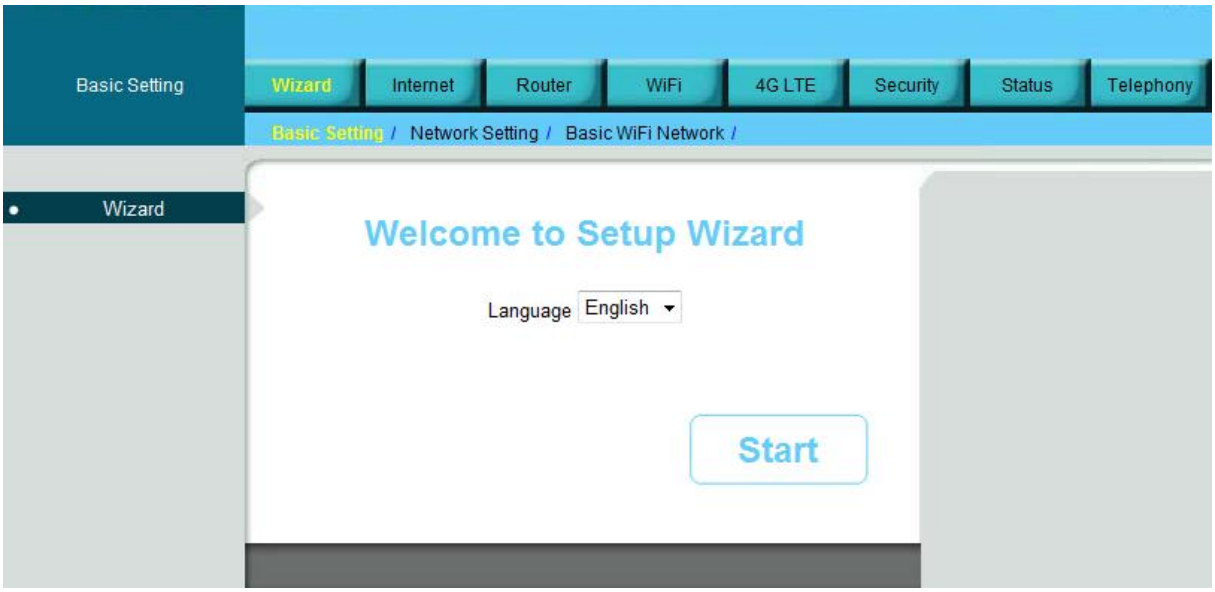


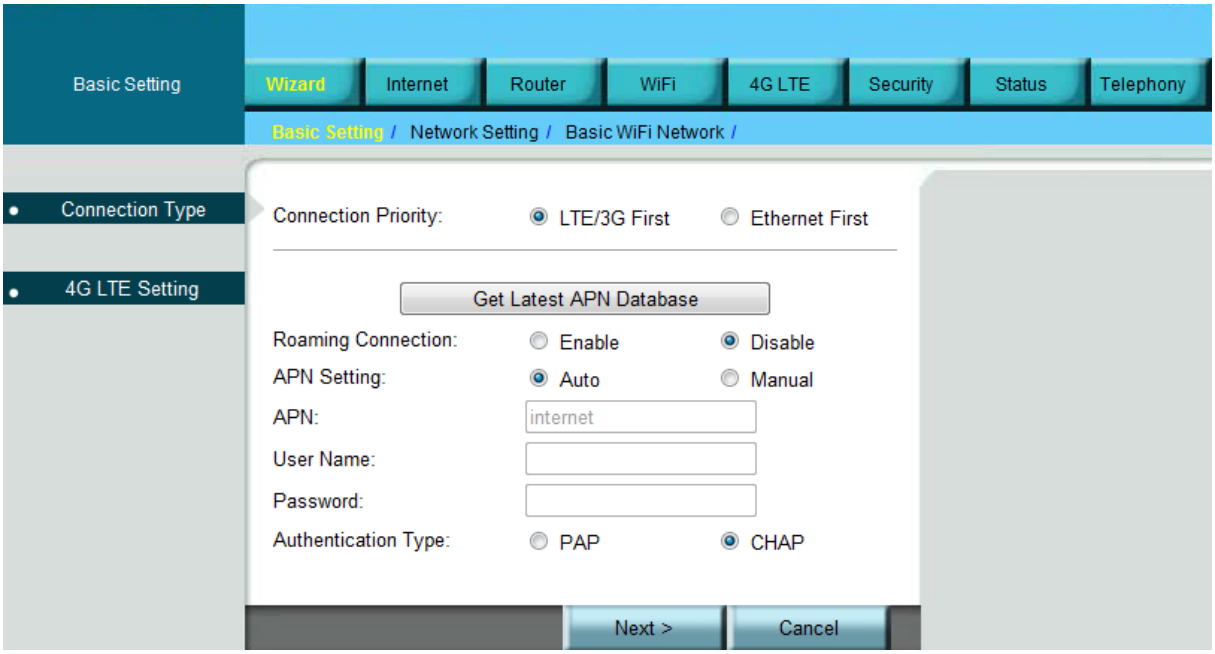
The screen automatically enters Screen Saver Mode after 60 seconds of inactivity. The Date and Time are displayed moving randomly on the screen. Short pressing the WPS key or any router state changes such as incoming VoIP call, LAN disconnect, etc. will bring the router out of Screen Saver Mode.

Wizard Setup

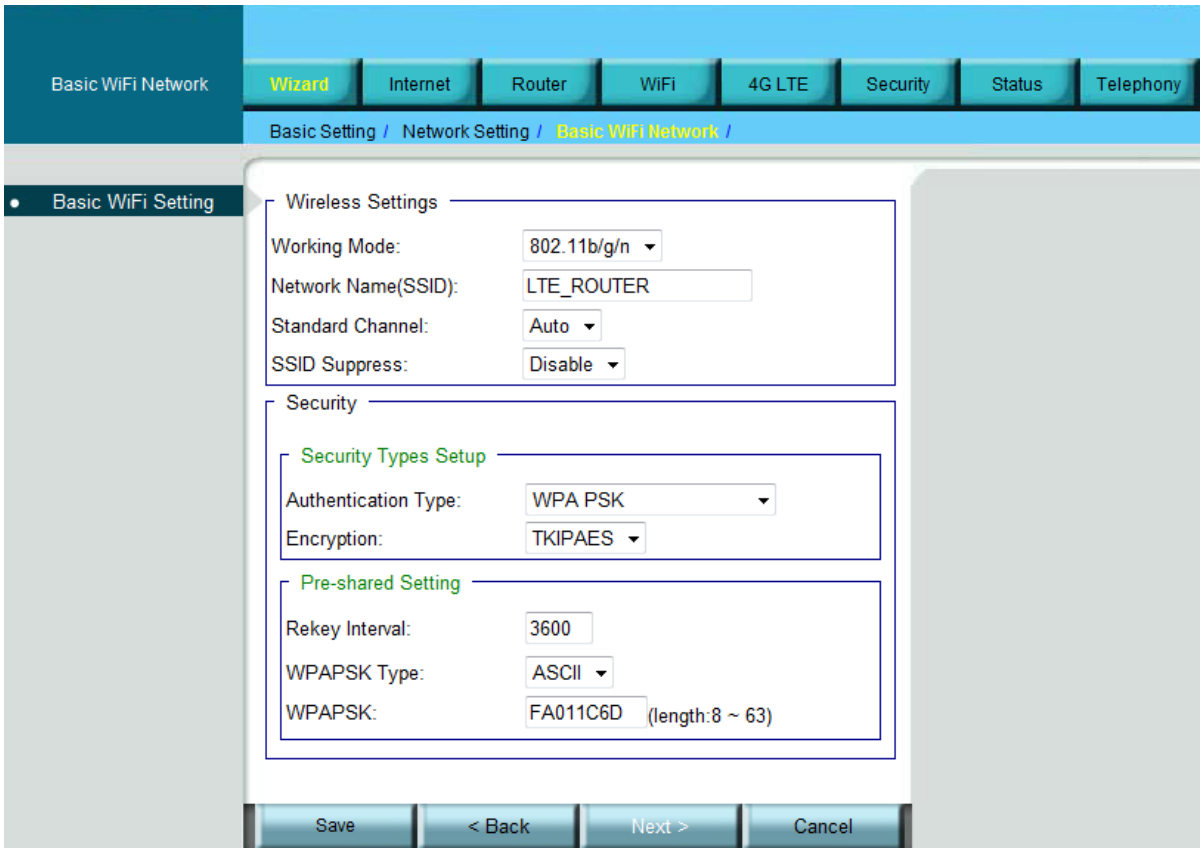
User can set preferred settings step by step via the Wizard.

User can select the preferred language and then set the Wizard via Basic Setting> Network Setting > Basic Wi-Fi Network.



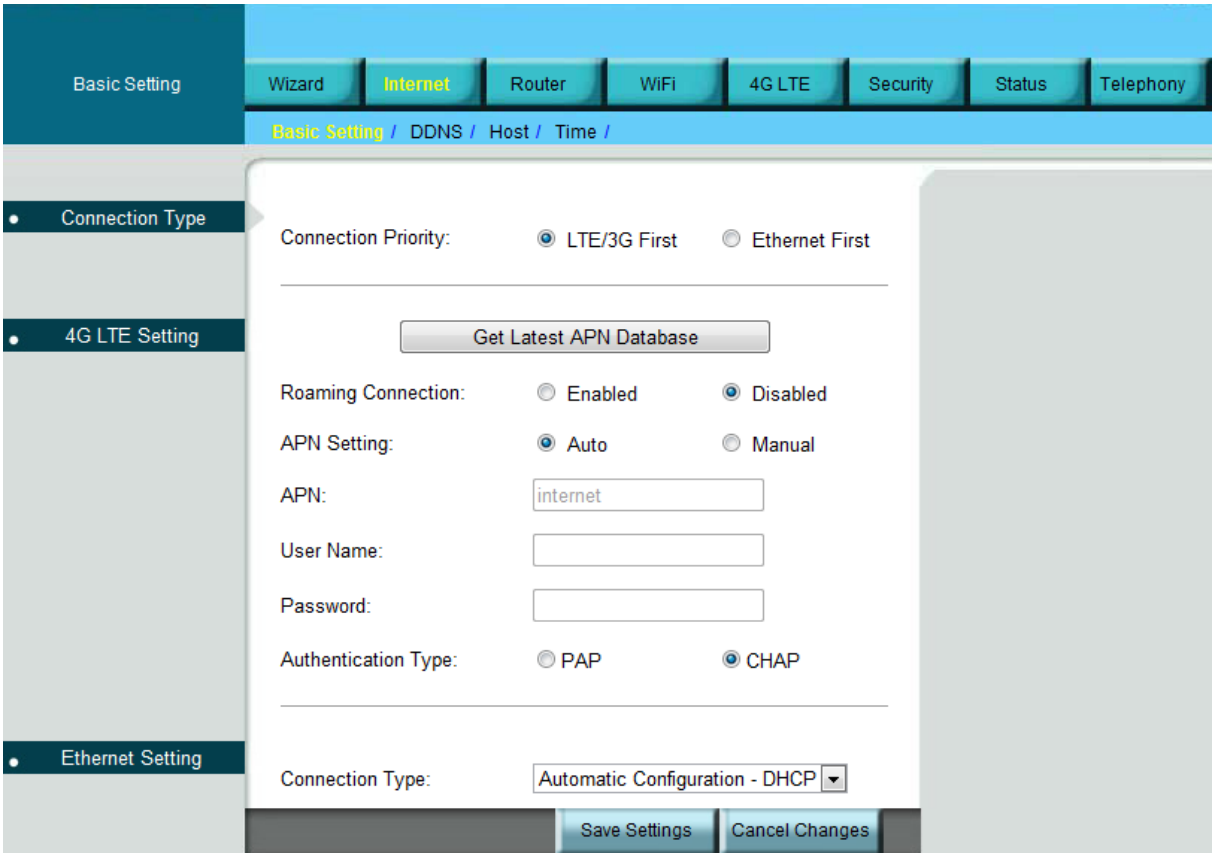


Network Setting
Wizard
Internet
Router
WiFi
4G LTE
Security
Status
Telephony
Basic Setting / Network Setting / Basic WiFi Network /
Router Access
Router Password:
Re-Enter to Confirm:
Router IP
Local IP Address: 192 . 168 . 1 . 1
Subnet Mask: 255.255.255.0
Device Name: R500.ROUTER
DHCP Service
DHCP Server: Enable Disable
DHCP Reservation
Start IP Address: 192 . 168. 1 . 2
Maximum Number of Users: 253
IP Address Range: 192 . 168 . 1 . 2 - 254
Client Lease Time: 15 minutes(0 means one day)
< Back
Next >
Cancel


Basic WiFi Network
Wizard
Internet
Router
WiFi
4G LTE
Security
Status
Telephony
Basic Setting / Network Setting / Basic WiFi Network /
Basic WiFi Setting
Wireless Settings
Working Mode: 802.11b/g/n
Network Name(SSID): LTE_ROUTER
Standard Channel: Auto
SSID Suppress: Disable
Security
Security Types Setup
Authentication Type: WPA PSK
Encryption: TKIPAES
Pre-shared Setting
Rekey Interval: 3600
WPAPSK Type: ASCII
WPAPSK: FA011C6D (length:8 ~ 63)
Save
< Back
Next >
Cancel

Internet Setup

Basic Setting



Connection Type

The Router can connect to the internet via either LTE/3G or Ethernet. Select the type of connection with higher priority. The selected type will be used for powering on the router when both types are available.

4G LTE Setting

Get Latest APN Database

Get the latest Profile Name, Number, User Name, Password, and APN from the web site automatically.

Roaming Connection

To allow roaming network connection, select **Enabled**. To block roaming connection, select **Disabled**.

> **Note:** Rates for roaming can be very high. Contact your mobile network operator for rates and more information.

APN Setting

The APN (Access Point Name) is provided by your mobile network operator. You can choose to set the APN automatically or manually. In most cases, the Router works properly when the APN is set to Auto.

To set the APN manually, contact your mobile network operator for the APN, User Name and Password of the data service.

Authentication Type

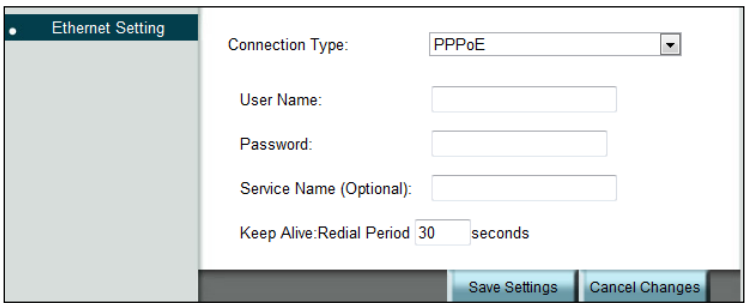
Select the type of authentication protocol used by your mobile network operator for data connections.

Ethernet Setting

Automatic Configuration - DHCP

Choose **Dynamic IP Address** to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for cable modem services.

PPPoE



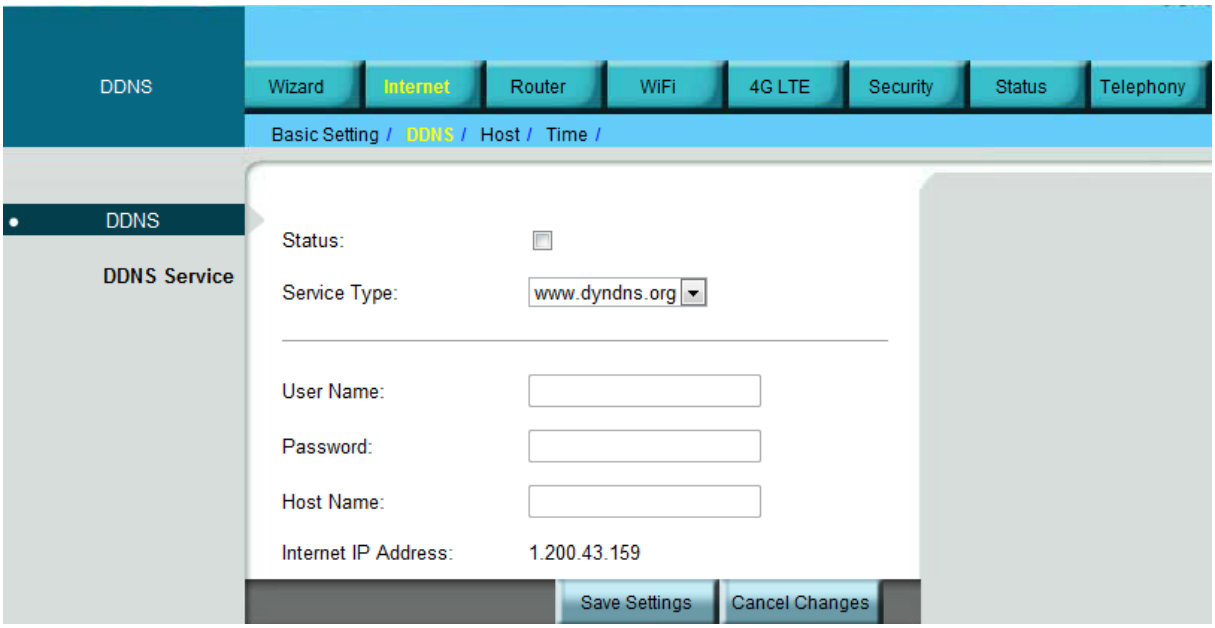
Choose **PPPoE** (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and

password. This option is typically used for DSL services.

Service Name: Enter the ISP Service Name (optional).

Keep Alive: The Router will periodically check your Internet connection. If you are disconnected, then the Router automatically tries to re-establish your connection. In the Redial Period field, specify how often you want the Router to check the Internet connection.

DDNS



DDNS (Dynamic Domain Name Service) is a system that allows the domain name data held in a name server to be updated in real time. It allows an Internet domain name to be assigned to a computer with a varying (dynamic) IP address. Before you can use this feature, you need to sign up for DDNS with a DDNS provider, www.dyndns.org or www.TZO.com.

Status: Check this box to enable or disable DDNS.

Service Type: From the drop-down list, select your DDNS service type.

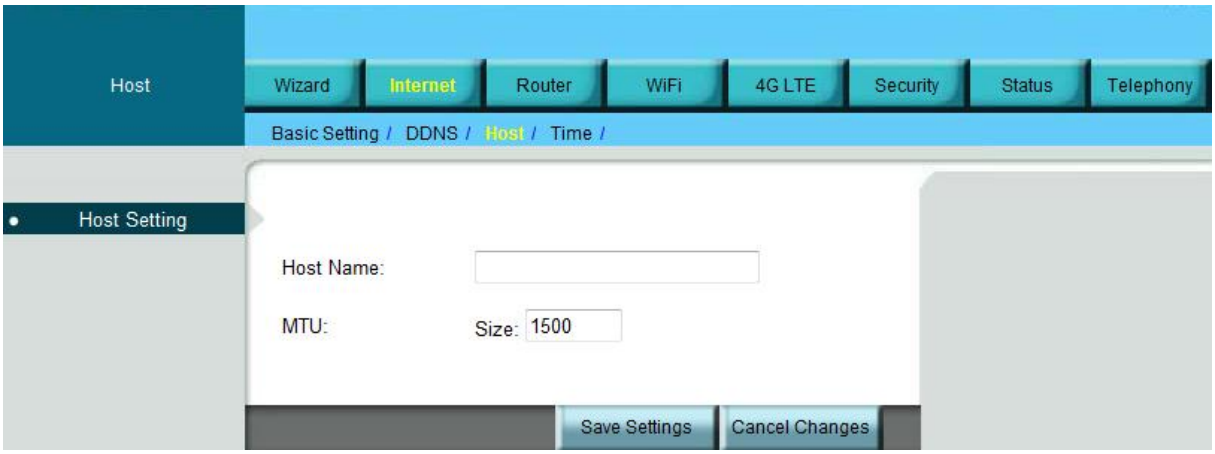
User name: Enter the user name for your DDNS account.

Password: Enter the password for your DDNS account.

Host name: The Host Name is optional but may be required by some ISPs.

Internet IP Address: The Router's Internet IP address is displayed here.

Host



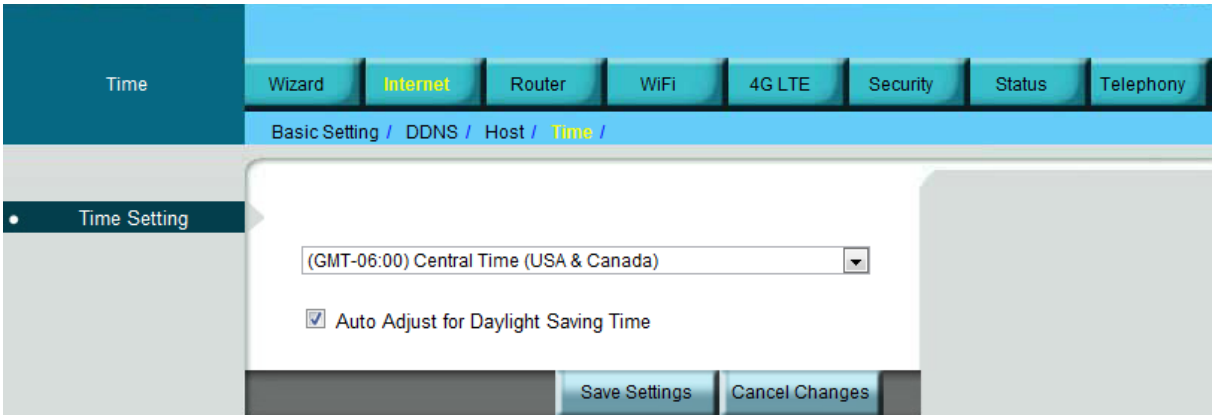
Host Name

This field allows you to assign a host name for the Router. Some ISPs require this name as identification. In most cases, leaving the fields blank will work.

MTU

MTU (Maximum Transmission Unit) specifies the largest packet size permitted for Internet transmission. To have the Router select the best MTU for your Internet connection, keep the default setting.

Time



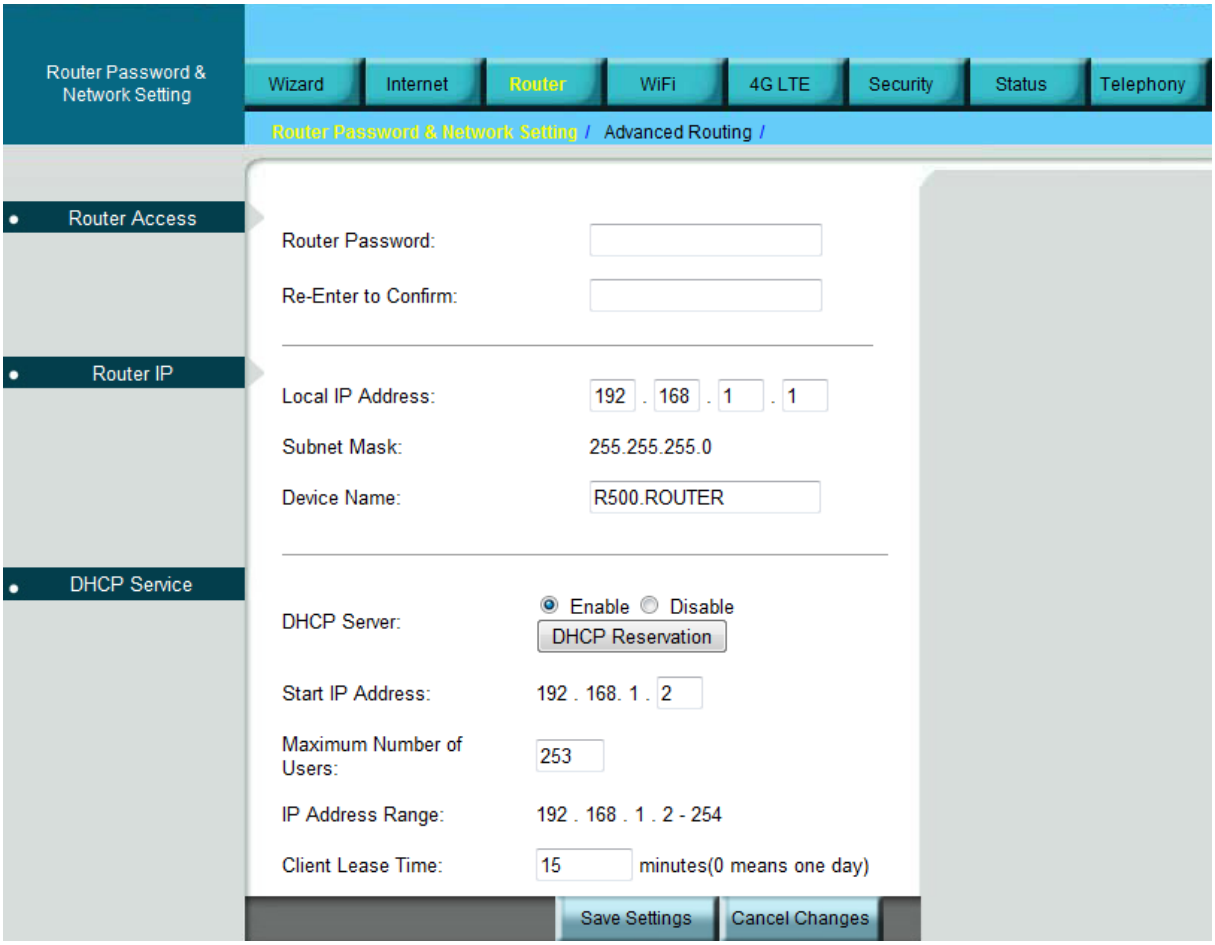
Time Setting

Select the Time Zone from the drop-down menu according to your current location.

Automatically adjust clock for daylight saving changes: Select the checkbox to enable Daylight Saving time.

Router Setup

Router password and Network setting



Router Access

You can change the Router's password here. Enter the password you want to set in the **Router Password** field, and re-enter it in the **Re-Enter to confirm** field. Then click **Save Settings**.

Router IP

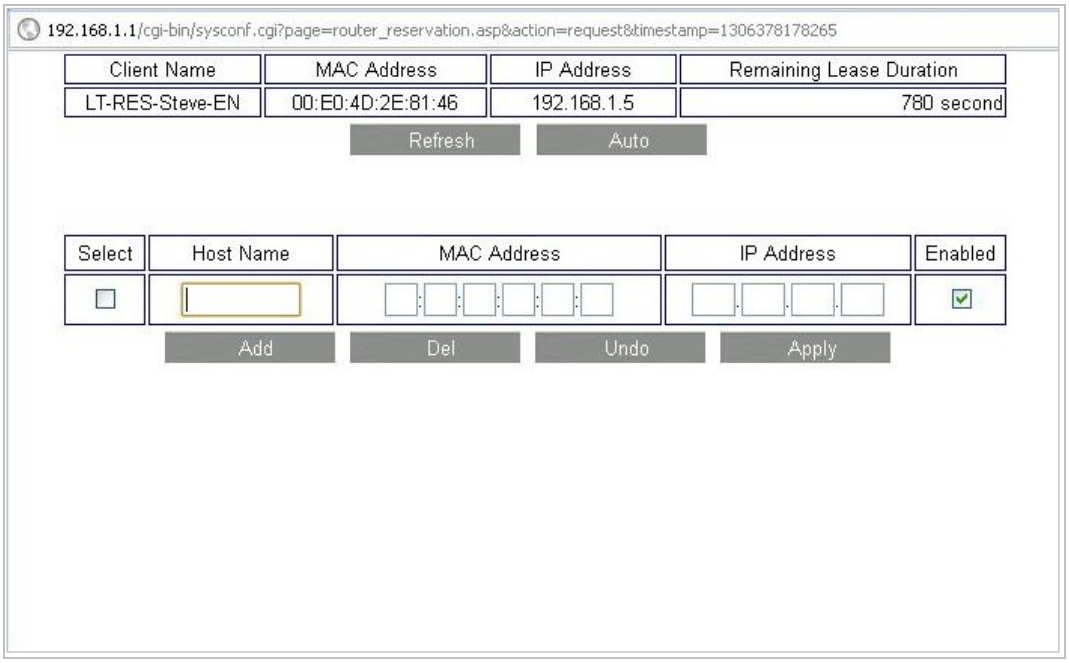
This is the Router's IP address and subnet mask which is seen in your local network. You may input the **Local IP Address** or **Device Name** to enter the WEB GUI of the router.

DHCP Service

DHCP stands for Dynamic Host Control Protocol. The DHCP Server will automatically assign an IP address to the computers on the LAN network. If the Router's DHCP server option is enabled, make sure there is no other DHCP server on your network.

DHCP Reservation

To assign the same IP address to a PC every time it reboots, click the **DHCP Reservation** button.



A list of DHCP clients is displayed with the following information: Client Name, MAC Address, IP Address, and Remaining Lease Duration.

To add clients:

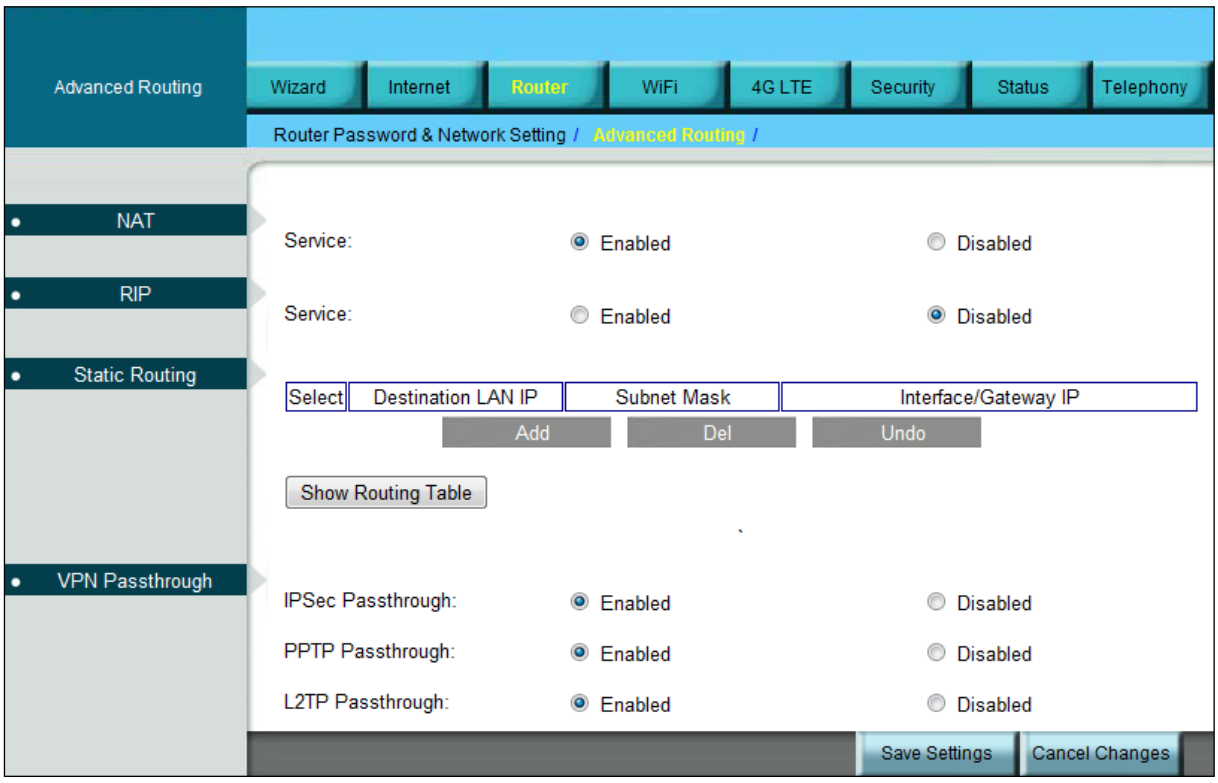
1. Click **Add**.
2. Enter the **Host Name**, **MAC Address** and **IP Address** of the client.
3. Activate/deactivate the **Enabled** checkbox to enable/disable the client's DHCP IP reservation.

To apply the changes, click **Apply**.

To cancel the latest changes without saving the changes, click **Undo**.

To delete a client, activate the appropriate checkbox in the **Select** column and click **Del**.

Advanced Routing



NAT Setup

The Network Address Translation (NAT) service is a standard that allows multiple computers on a private network to share a single public IP address.

RIP

The **Routing Information Protocol (RIP)** helps the Router dynamically adapt to changes of network routes by communicating information about which networks each Router can reach and how far away those networks are.

Static Routing

This section allows you to define fixed routes to defined destinations.

To add a new static route:

1. Click **Add**.
2. In the **Destination LAN IP** field, enter the Destination IP address that will be assigned to a specific network or host.
3. In the **Subnet Mask** field, enter the subnet mask associated with the Destination IP.
4. In the **Interface/Gateway IP** field, click on the drop down list to configure the IP value for the **IP**, **LAN & Wireless**, and **Internet**. **IP** is the address of the gateway device that allows for contact between the Router and the remote network or host. **LAN & Wireless** and **Internet** indicates whether the Destination IP is on the local network (**LAN & Wireless**) or WAN (**Internet**).

To apply the changes, click **Save Settings**.

To cancel the latest changes without saving the changes, click **Undo**.

To delete a client, activate the appropriate checkbox in the **Select** column and click **Del**.

VPN Passthrough

A **Virtual Private Network (VPN)** is a type of secured private network connection, built upon publicly-accessible infrastructure such as the Internet.

IPSec Passthrough

IP Security (IPSec) provides authentication and encryption. Since it is mainly a Layer 3 technology, it can secure all data on the network.

PPTP Passthrough

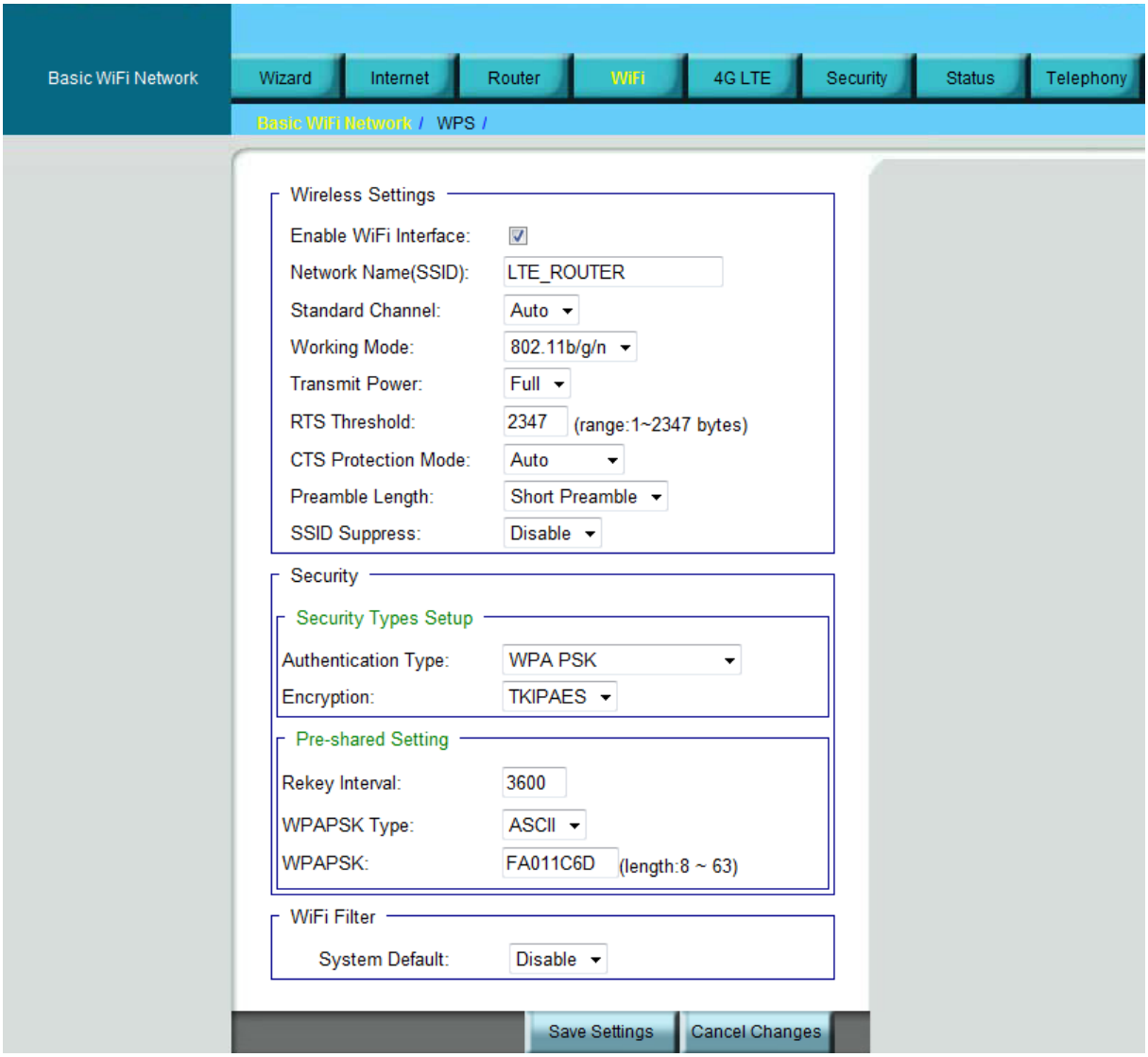
Point-to-Point Tunneling Protocol (PPTP) allows you to establish virtual private networks.

L2TP Passthrough

Layer 2 Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol and is also used to establish virtual private networks.

WiFi Setup

Basic WiFi Network



Basic WiFi Network

Wireless Settings

Enable WiFi Interface: Select this option to enable the WiFi feature on the router.

Network Name (SSID): Network Name is used for identifying the Wireless LAN (WLAN).

Standard Channel: The radio channel number. The permissible channels depend on the Regulatory Domain (e.g in the USA, it is 1 to 11).

Working Mode: From this drop-down menu, you can select the type of wireless standard for your WiFi network.

Transmit Power: The power level for WiFi transmission to be used by the router.

RTS Threshold: This value should remain at its default setting. If inconsistent data flow is a problem, only a minor modification should be made.

CTS Protection Mode: CTS (Clear To Send) is a function used to minimize collisions among wireless devices on a wireless local area network (WLAN). The default setting is **Auto** and the Router automatically uses CTS Protection Mode when your Wireless-G products are experiencing severe problems and are not able to transmit to the Router in an environment with heavy traffic. This function boosts the Router's ability to catch all Wireless-B and Wireless-G transmissions, but it severely decreases performance.

Preamble Length: The preamble is used by the client PC receiver to acquire the wireless signal and synchronize with the router's transmitter. The router supports **Long Preamble** and **Short Preamble**. Selecting **Long Preamble** results in longer preamble transmission times yet supports legacy 802.11 systems. **Short Preamble** reduces the preamble transmission time but is not compatible with legacy 802.11 systems. The default setting, **Short Preamble**, should be used unless you are experiencing WiFi problems such as frequent disconnects, slow upload/download along with a low signal strength.

SSID Suppress: For security purposes, you may choose to hide your network's SSID by selecting **Enable** from the drop-down list. This will prevent computers scanning for the presence of wireless networks to detect your network name.

Security

Authentication Type: Allows you to configure the authentication method used to the router to authenticate clients. The router supports the following authentication types: **Open System, 802.1x, Shared Key, WPA, WPA2, WPA-WPA2-Mixed, WPA PSK, WPA2 PSK, WPA-WPA2-Mixed PSK.**

Encryption: Select the type of encryption on the data that is transmitted between the router and the clients. The router supports the following authentication types: **WEP, TPIK, AES, TPIKAES.**

Open System

This wireless standard uses no authentication.
Encryption: Choose **NONE or WEP** from the drop down list.

WEP: The Router supports two WEP (Wired Equivalent Privacy) standards: 64-bit and 128-bit. Select a standard from the drop-down list. The 64-bits encryption requires 10 hexadecimal digits (letters a-f and numbers 0-9 are valid). The 128-bits encryption requires 26 hexadecimal digits (letters a-f and numbers 0-9 are valid).You can set up to four different keys.

802.1x

IEEE 802.1x is an authentication system for devices connecting to a WiFi network. This system requires the use of an authentication server that is part of the network.

Encryption: Only **WEP** is available.

Rekey Interval: Enter a key renewal value to tell the Router how often it should change the encryption keys.

RADIUS stands for Remote Authentication Dial-In User Service. It is a networking protocol that uses access servers to provide centralized management of access to large networks.

RADIUS Server: Enter the IP Address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server..

RADIUS Key: Enter the key shared between the Router and the server.

Shared Key

An authentication system that uses a simple challenge/response protocol with a WEP key.

Encryption: Only **WEP** is available.

WPA

WPA, or WiFi Protected Access, is a WiFi standard that was designed to improve the security features of WEP. WPA uses two encryption methods, TKIP and AES, with dynamic keys. This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption: Choose **TKIP, AES, TKIPAES** from the drop down list. AES is a stronger encryption method than TKIP. TKIPAES uses either TKIP or AES during the connection.

Rekey Interval: Enter a key renewal value to tell the Router how often it should change the encryption keys..

RADIUS Server: Enter the IP Address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server.

RADIUS Key: Enter the key shared between the Router and the server.

WPA2

WPA2 is a more advanced, more secure version of WPA. This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption: Choose **TKIP, AES, TKIPAES** from the drop down list.

Rekey Interval: Enter a key renewal value to tell the Router how often it should change the encryption keys.

RADIUS Server: Enter the IP Address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server.

RADIUS Key: Enter the key shared between the Router and the server.

WPA - WPA2 - Mixed

WPA and WPA2 Mixed means the router uses both WPA and WPA2 for authentication and allows the client PC to choose between the two methods. This option features WPA used in coordination with a RADIUS server. (This should only be used when a RADIUS server is connected to the Router.)

Encryption: Choose **TKIP, AES, TKIPAES** from the drop down list.

Rekey Interval: Enter a key renewal value to tell the Router how often it should change the encryption keys.

RADIUS Server: Enter the IP Address of the RADIUS server.

RADIUS Port: Enter the port number of the RADIUS server.

RADIUS Key: Enter the key shared between the Router and the server.

WPA PSK

Also known as WPA Personal, this authentication system does not require

the use of a RADIUS authentication server.

Encryption: Choose **TKIP, AES, TKIPAES** from the drop down list.

Rekey Interval: Enter a key renewal value to tell the Router how often it should change the encryption keys.

WPAPSK Type: Choose **ASCII** or **HEX** from the drop down list.

WPAPSK: Enter the key shared between the Router and the server. If **ASCII** is chosen as the **WPAPSK Type**, enter a passphrase between 8-63 characters. For **Hex**, enter a string of 64 hexadecimal digits.

WPA2 PSK

WPA2 PSK is a more advanced, more secure version of WPA PSK.

Encryption: Choose **TKIP, AES, TKIPAES** from the drop down list.

Rekey Interval: Enter a key renewal value to tell the Router how often it should change the encryption keys.

WPAPSK Type: Choose **ASCII** or **HEX** from the drop down list.

WPAPSK: Enter the key shared between the Router and the server. If **ASCII** is chosen as the **WPAPSK Type**, enter a passphrase between 8-63 characters. For **Hex**, enter a string of 64 hexadecimal digits.

WPA - WPA2 - Mixed PSK

WPA and WPA2 Mixed PSK means the router uses both WPA PSK and WPA2 PSK for authentication and allows the client PC to choose between the two methods.

Encryption: Choose **TKIP, AES, TKIPAES** from the drop down list.

Rekey Interval: Enter a key renewal value to tell the Router how often it should change the encryption keys.

WPAPSK Type: Choose **ASCII** or **HEX** from the drop down list.

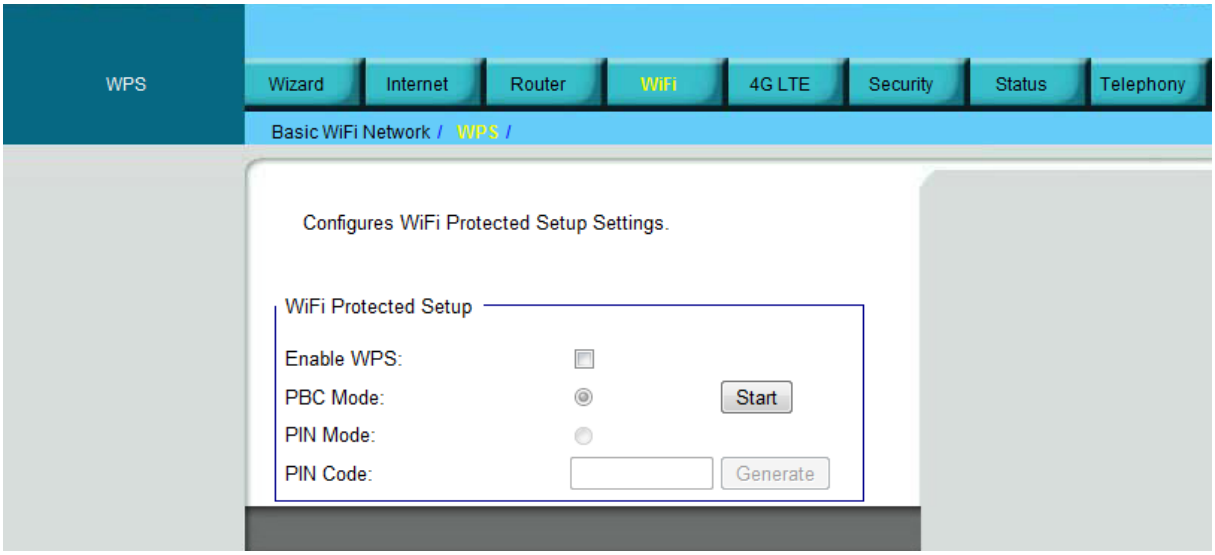
WPAPSK: Enter the key shared between the Router and the server. If **ASCII** is chosen as the **WPAPSK Type**, enter a passphrase between 8-63 characters. For **Hex**, enter a string of 64 hexadecimal digits.

WiFi Filter

You can allow or deny specific users access to your wireless network by using the WiFi Filter. Allow a specific user to your wireless network by selecting **Allow** under the drop down list and entering the appropriate MAC address; similarly, deny a specific user from your network by

selecting **Deny** and entering the appropriate MAC address.

▪ WPS



Wi-Fi Protected Setup (WPS) is a standard designed to easily setup and automatically configure secure Wi-Fi networks between two WPS supported devices. If the client PC supports WPS, the WPS feature can be a user-friendly and simple process to get your Wi-Fi network up and running.

Enable WPS: This enables the WPS feature on the router.

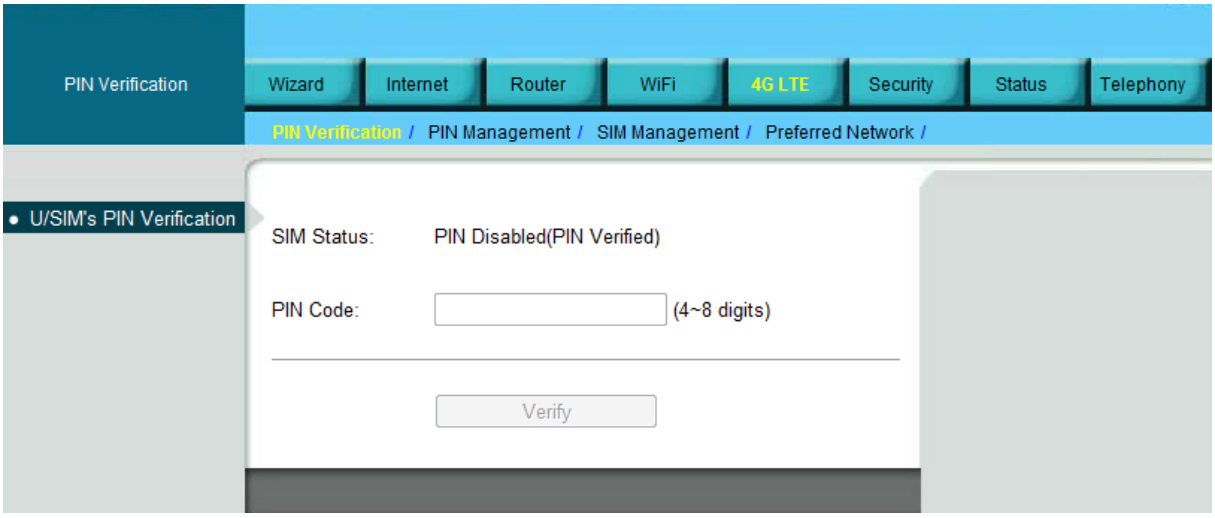
To initiate a WPS session between the router and the prospective client PC, select either the PBC (Push-Button Configuration) Mode or PIN Mode and click on the **Start** button. The client PC will have 2 minutes to connect to the router before the current session times out.

PBC Mode: This mode allows the WPS session to be configured simply by pressing the **Start** button on the web and on the client PC. Alternatively, you can also press the WPS button on the side of router to initiate a session.

PIN Mode: This mode uses a PIN code to configure the WPS session between the router and the client PC. Enter a PIN code (maximum 8 digits consisting of 0-9) or click **Generate** to automatically generate a random 8 digit number. The PIN entered on the client PC must match this PIN code for a successful WPS configuration.

4G LTE Setup

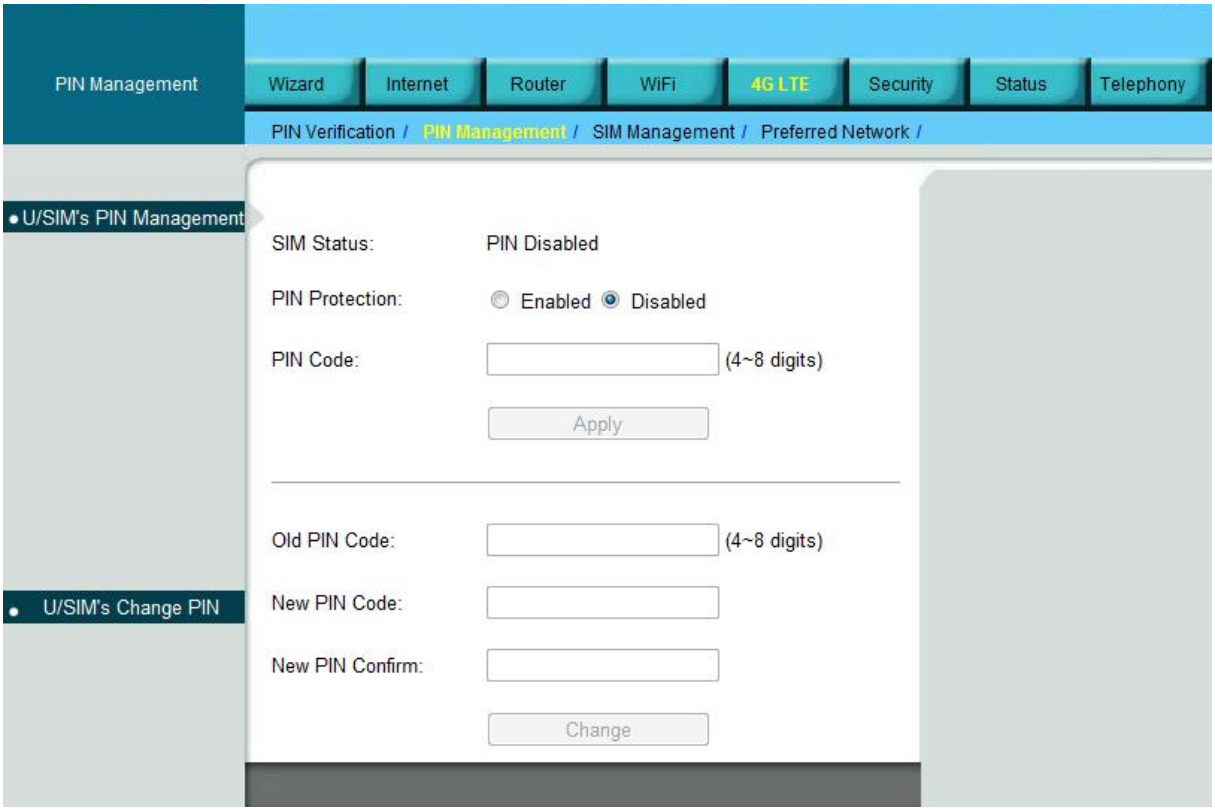
PIN Verification



U/SIM's PIN Verification

If your SIM card PIN protection is enabled, you must enter the PIN code for verification. Enter the code in the PIN Code field, and click **Verify**.

PIN Management



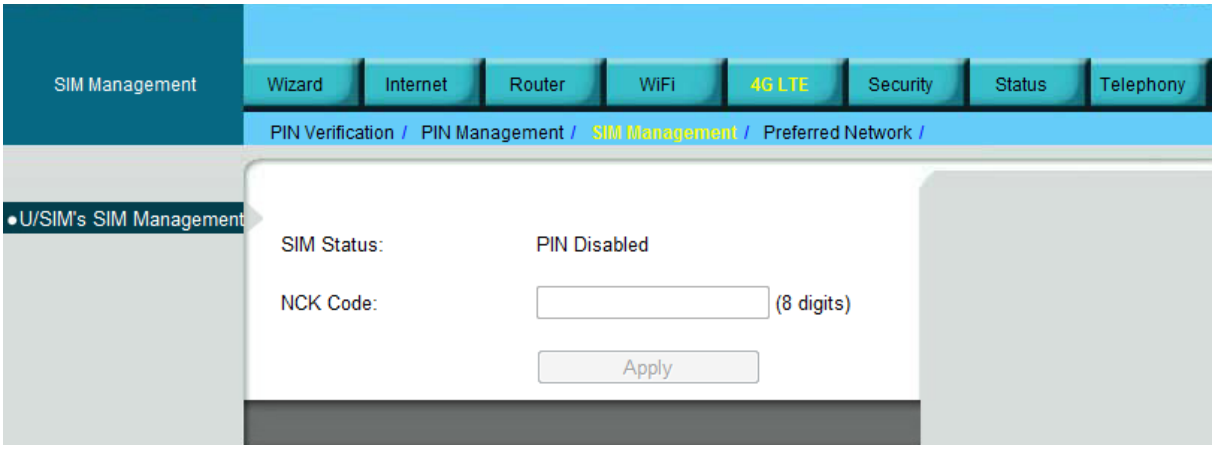
U/SIM's PIN Management

After your SIM card is verified, you can enable or disable the PIN protection on your SIM card. Select **Enabled** or **Disabled**, and click **Apply**.

U/SIM's Change PIN

You can change the PIN code on the SIM card. Enter your original PIN code in the **Old PIN Code** field, enter the new PIN code in the **New PIN Code** field and the **New PIN Confirm** field, and click **Change**.

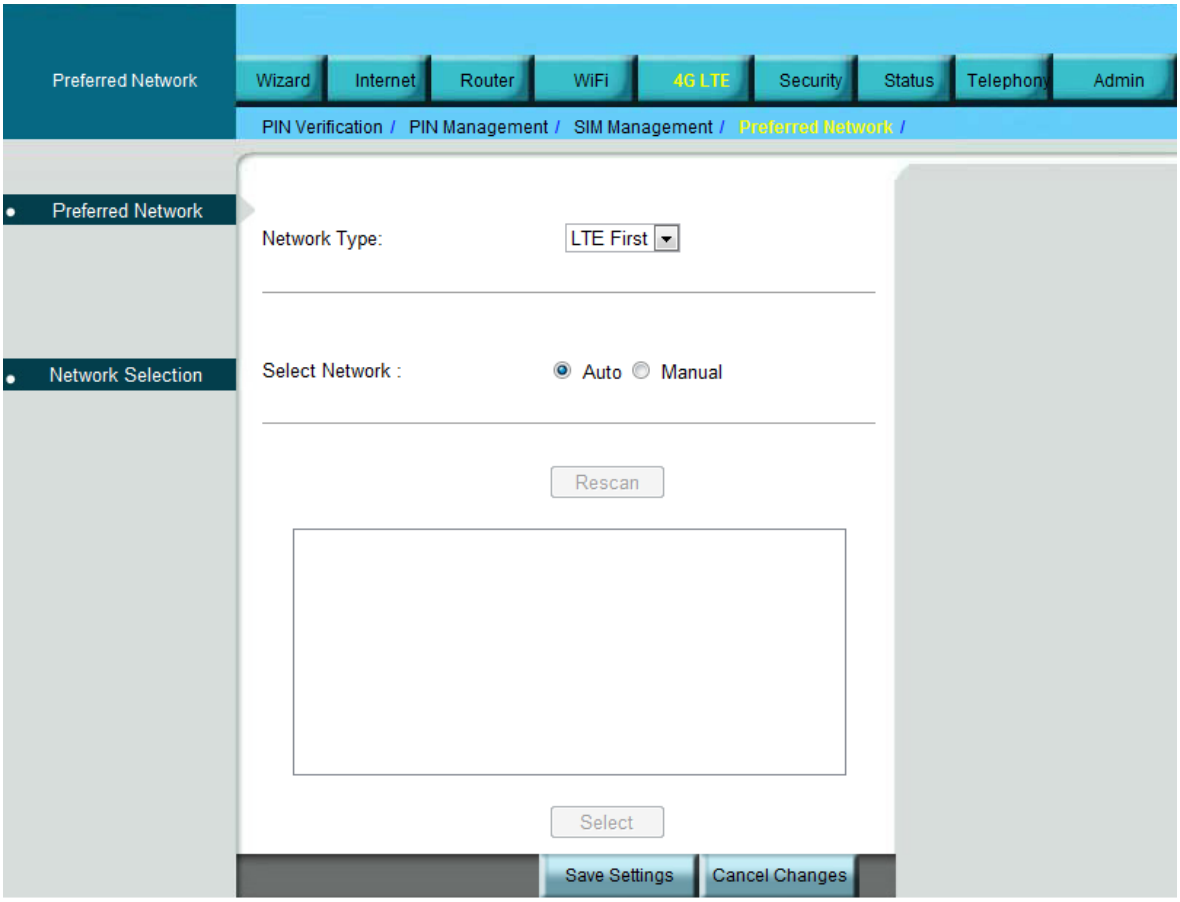
SIM Management



U/SIM's SIM Management

If the router has SIM lock function, you are not allowed to use the ISP SIM which is not in the SIM locked list. You may input the NCK code to unlock it. Please contact your ISP for further information.

Preferred Network



Preferred Network

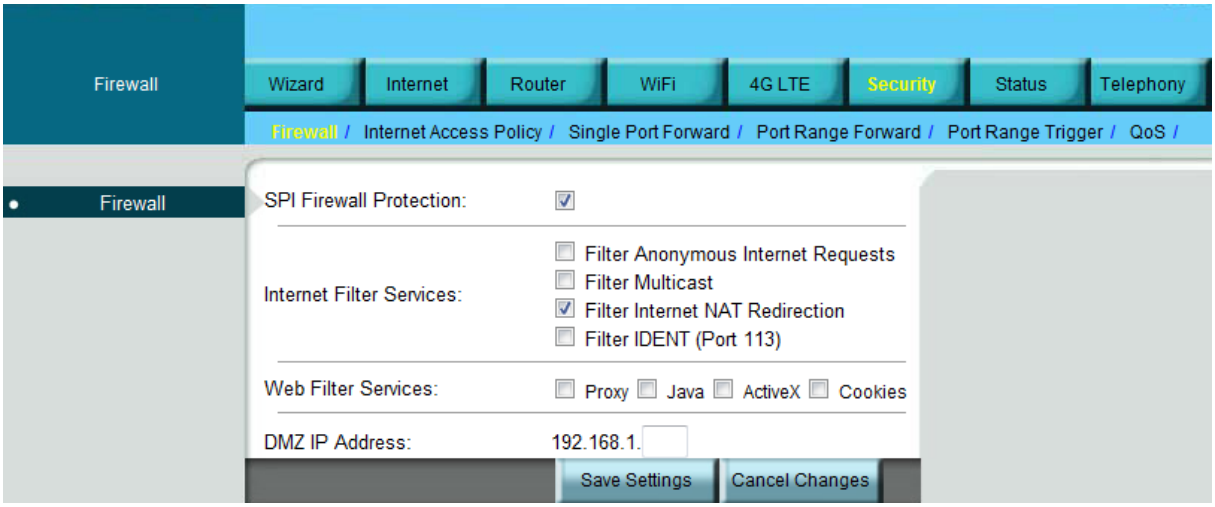
Network Type: In the drop-down menu, select the network type your SIM card supports. The available network types are automatically detected when you insert your SIM card. If you do not know the network type, select **LTE First**.

Network Selection

To select the mobile network operator automatically, in the **Select Network** field, select **Auto**. To select the operator from a list, select **Manual** and click **Rescan**. The list is displayed below. Select the mobile network operator you wish to use on your SIM card.

Security Setup

Firewall



Firewall

This tab is used to configure a firewall that filters out various types of unwanted traffic on the Router's local network.

SPI Firewall Protection

The SPI (stateful packet inspection) firewall is programmed to recognize legitimate packets for different types of connections. Only packets matching a known connection state will be allowed by the firewall; others will be rejected.

Internet filter services

Filter Anonymous Internet Requests: This feature makes it more difficult for outside users to work their way into your network.

Filter Multicast: Multicasting allows for multiple transmissions to specific recipients at the same time. If multicasting is permitted, the Router allows IP multicast packets to be forwarded to the appropriate computers.

Filter Internet NAT Redirection: To prevent local computers from using public IP addresses to access local servers, select **Filter Internet NAT Redirection**.

Filter IDENT (Port 113): This feature keeps port 113 from being scanned by devices outside of your local network.

Web filter services

Using the Web Filters feature, you may enable up to four specific filtering methods.

Proxy: Use of WAN proxy servers may compromise the Router's security. Select this option to disable access to any WAN proxy servers.

Java: Java is a programming language for websites. Select this option to disable Java. If you disable Java, you run the risk of not having access to Internet sites created using this programming language.

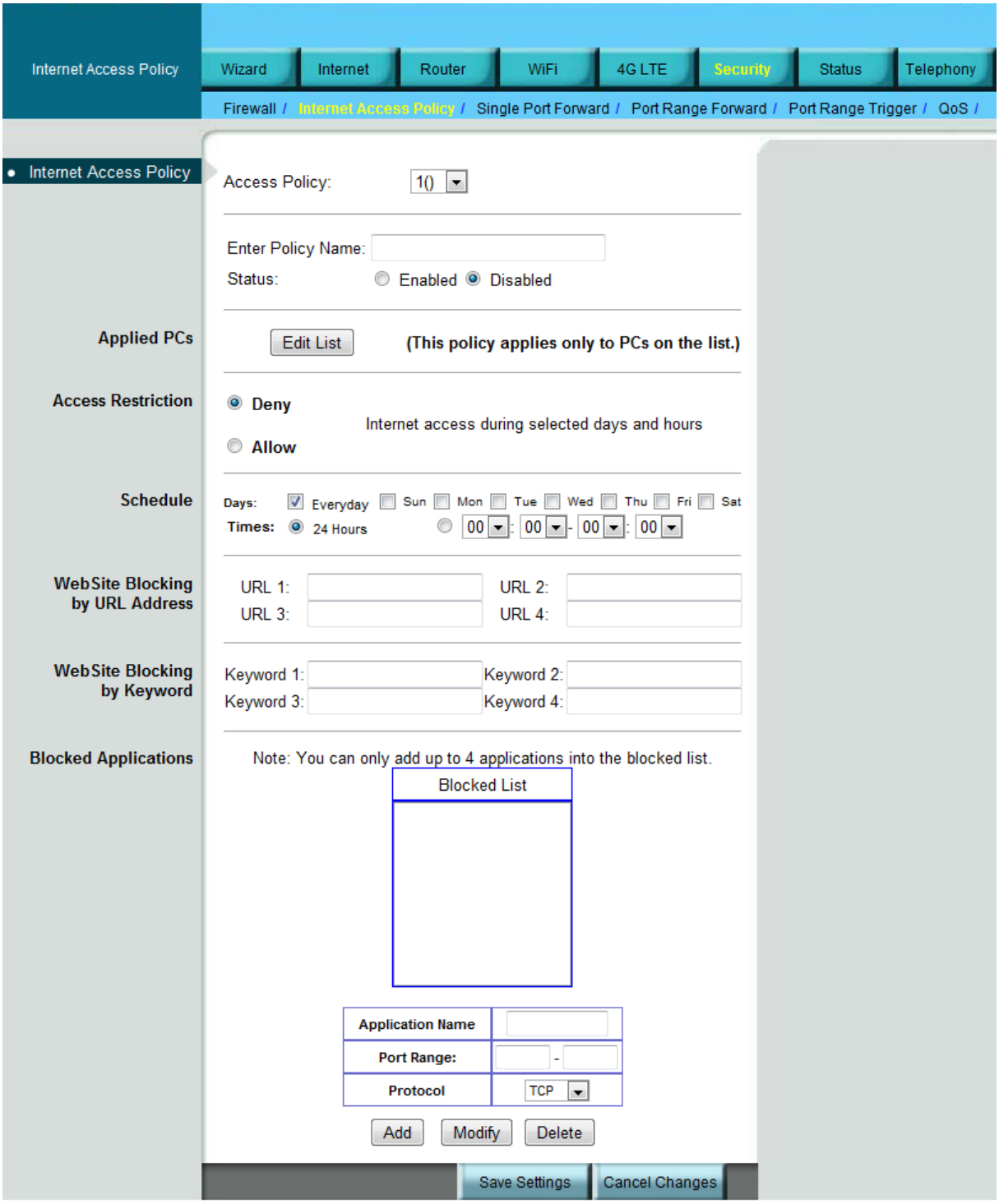
ActiveX: ActiveX is a programming language for websites. Select this option to disable ActiveX. If you disable ActiveX, you run the risk of not having access to Internet sites created using this programming language.

Cookies: A cookie is data stored on your PC and used by Internet sites when you interact with them. Select this option to disable cookies.

DMZ IP Address

When a firewall is used, it is sometimes necessary to place some clients (for example Internet games, video conferencing, or VPN connections) outside of the firewall while leaving the others protected. You can do this using a Demilitarized Zone. This feature allows you to specify the IP address of the computers that are placed outside the firewall of your network.

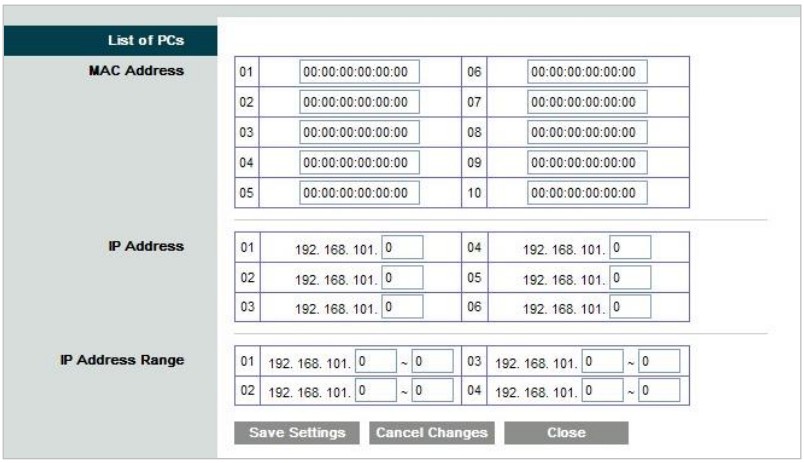
Internet Access Policy



Access can be managed by a policy. Use the settings on this screen to establish and access policies. To display a policy's settings, select the policy from the drop-down menu.

To create an Internet access policy:

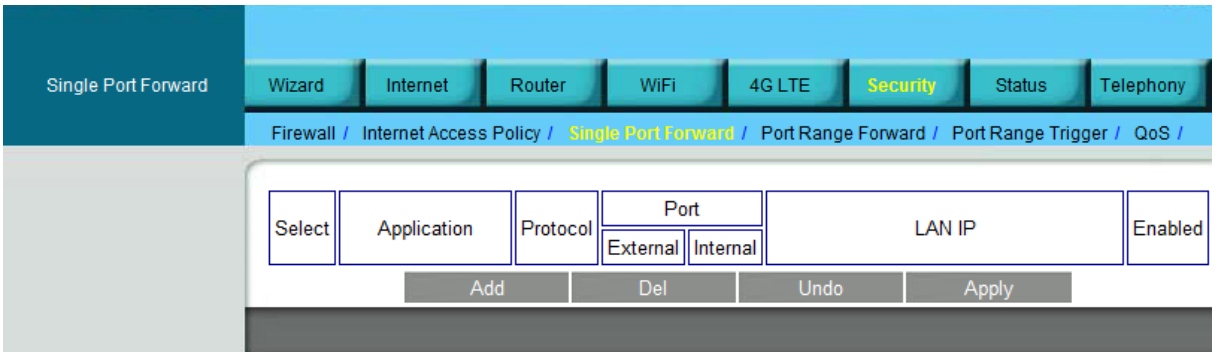
1. Select a number from the **Access Policy** dropdown menu.
2. Enter a policy name in the field provided.
3. To enable the policy, select **Enabled**.



4. To select which PCs are affected by the policy, click **Edit List**. The List of PCs screen appears. You can select a PC by MAC Address or IP Address. You can also enter a range of IP Addresses if you want the policy to affect a group of PCs. After making your changes, click **Save Settings** to apply your changes or **Cancel Changes** to cancel your changes. Then click **Close**.
5. Select the appropriate option, **Deny** or **Allow**, depending on whether you want to block or allow Internet access for the PCs you listed on the List of PCs screen. If **Deny** is selected, the PCs listed are not allowed to access the Internet under the current policy. If **Allow** is selected, the PCs listed are blocked some the Internet under the current policy. PCs that are not listed under the policy are allowed to access the Internet.
6. Decide which days and what times you want this policy to be enforced. Select the individual days during which the policy will be in effect, or select **Everyday**. To set times for the policy, select **24 Hours**, and enter the times you want.
7. To filter websites by URL, enter URLs in the **Website Blocking by URL Address** fields. To filter websites by keywords, enter keywords in the **Website Blocking by Keyword** fields.
8. To filter access to various services accessed over the Internet, such as FTP or telnet, add an application into **Blocked Applications**. (You can

only add up to 4 applications.) Enter the information in the **Application Name** and **Port Range** fields and select the **Protocol** type, then click **Add**. To modify an existing application, select the application from the Blocked List, make the appropriate changes and click **Modify**. To delete an existing application from the Blocked List, select the application and click **Delete**.

▪ Single Port Forward



Single Port Forwarding

Port Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications.

To forward a single port:

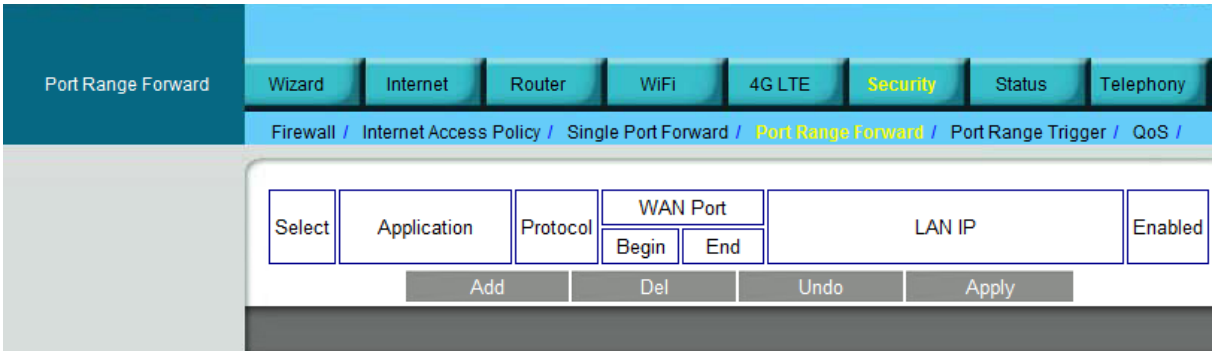
1. Click **Add**.
2. In the **Application** field, enter the name of your application.
3. In the **Protocol** field, select the protocol used for this application: TCP, UDP, or Both.
4. In the **Port (External)** field, enter the port number of the external port used by the server or Internet application.
5. In the **Port (Internal)** field, enter the port number of the internal port used by the server or Internet application.
6. In the **LAN IP** field, enter the IP address of the PC running the specific application.
7. Activate/deactivate the **Enabled** checkbox to enable/disable the client's DHCP IP reservation.

To apply the changes, click **Apply**.

To cancel the latest changes without saving the changes, click **Undo**.

To delete a port forwarding rule, activate the appropriate checkbox in the **Select** column and click **Del**.

Port Range Forward



Port Range Forwarding

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, and other specialized Internet applications.

To forward a port range:

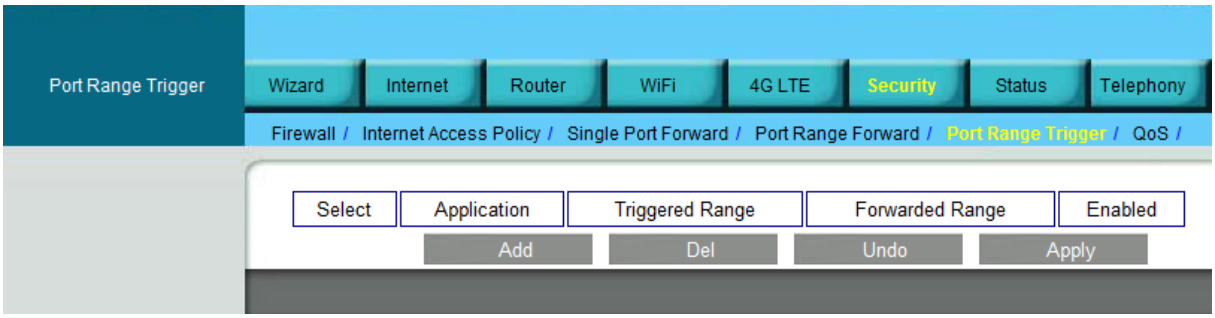
1. Click **Add**.
2. In the **Application** field, enter the name of your application.
3. In the **Protocol** field, select the protocol used for this application: TCP, UDP, or Both.
4. In the **WAN Port (Begin)** field, enter the beginning port number used by the server or Internet application.
5. In the **WAN Port (End)** field, enter the end port number used by the server or Internet application.
6. In the **LAN IP** field, enter the IP address of the PC running the specific application.
7. Activate/deactivate the **Enabled** checkbox to enable/disable the client's DHCP IP reservation.

To apply the changes, click **Apply**.

To cancel the latest changes without saving the changes, click **Undo**.

To delete a port forwarding rule, activate the appropriate checkbox in the **Select** column and click **Del**.

Port Range Trigger



Port Range Triggering

This feature allows the Router to watch outgoing data for specific port numbers. The Router remembers the IP address of the computer that sends the matching data, so that when the requested data returns through the Router, the data is pulled back to the proper computer by way of IP address and port mapping rules.

To add a new port range triggering:

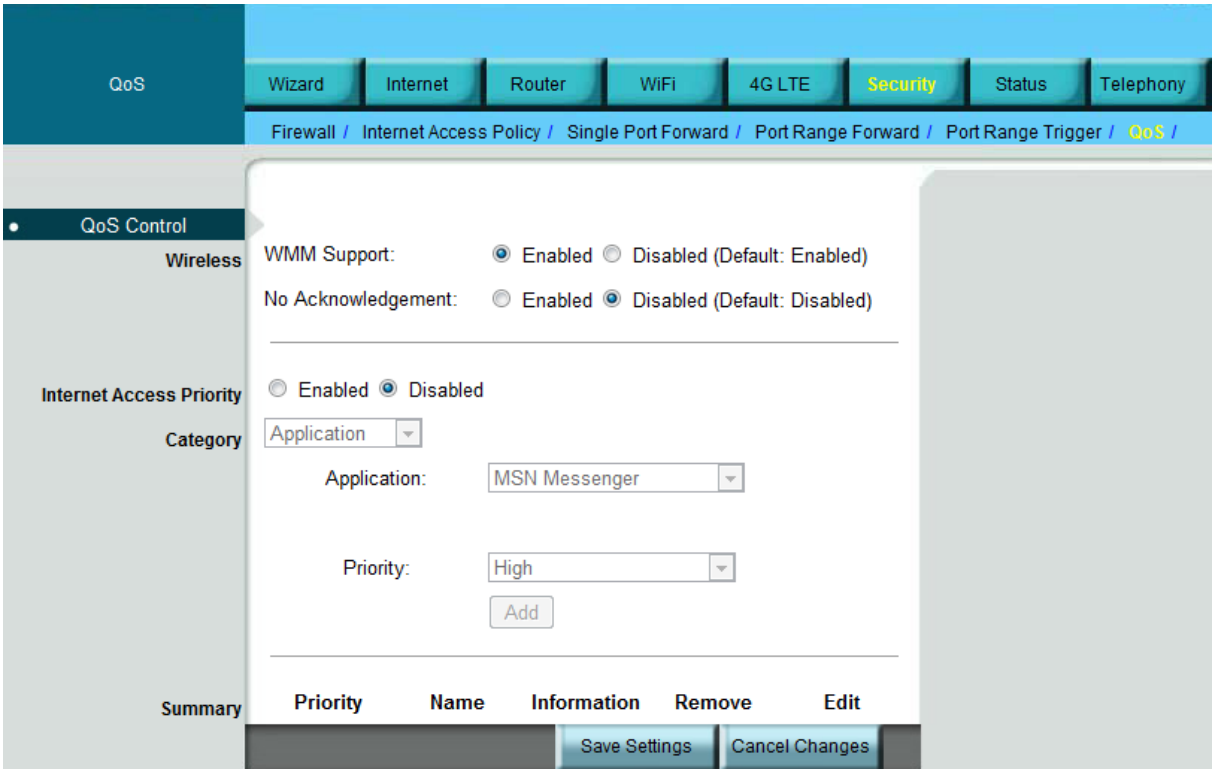
1. Click **Add**.
2. In the **Application** field, enter the name of your application.
3. In the **Triggered Range** field, enter the triggered port number range for each application. Check with the Internet application documentation for the port number needed. Enter the starting port number of the Triggered Range in the left field. Enter the ending port number of the Triggered Range in the right field.
4. In the **Forwarded Range** field, enter the forwarded port number range for each application. Check with the Internet application documentation for the port number needed. Enter the ending port number of the Triggered Range in the right field.
5. Activate/deactivate the **Enabled** checkbox to enable/disable the client's DHCP IP reservation.

To apply the changes, click **Apply**.

To cancel the latest changes without saving the changes, click **Undo**.

To delete a port triggering rule, activate the appropriate checkbox in the **Select** column and click **Del**.

QoS



QoS Control

Quality of service is the ability to provide different priorities to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

Wireless

WMM Support: If no devices on your network support WMM, select **Disabled**. Otherwise, keep the default, **Enabled**.

No Acknowledgement: If the Router's Acknowledgement feature is disabled, the Router will not re-send data if an error occurs, select the default, **Disabled**. Otherwise, select **Enabled**.

Internet Access Priority

You can set the Internet bandwidth priority for a variety of applications and devices. There are four levels priority: **High**, **Medium**, **Normal**, and **Low**. To use the Internet Access policies you set, select **Enabled**.

Category

There are four categories available. Select one of the categories and proceed to the instructions for your selection.

To add an online games or applications:

1. Select the appropriate online games or applications.
2. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.
3. Click **Add** to save your changes.

To add a new online games or applications:

1. Select **Add a new Application**.
2. Enter any name to indicate the name of the entry.
3. Enter the port range that the application will be using. You can have up to three ranges to define for this bandwidth allocation. Port numbers can range from 1 to 65535.
4. Select the protocol **TCP** or **UDP**, or select **Both**.
5. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.
6. Click **Add** and **Save Settings** to save your changes.

To add an MAC address:

1. Enter a name for your device.
2. Enter the MAC address of your device.
3. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.
4. Click **Add** and **Save Settings** to save your changes.

To add a Voice Device:

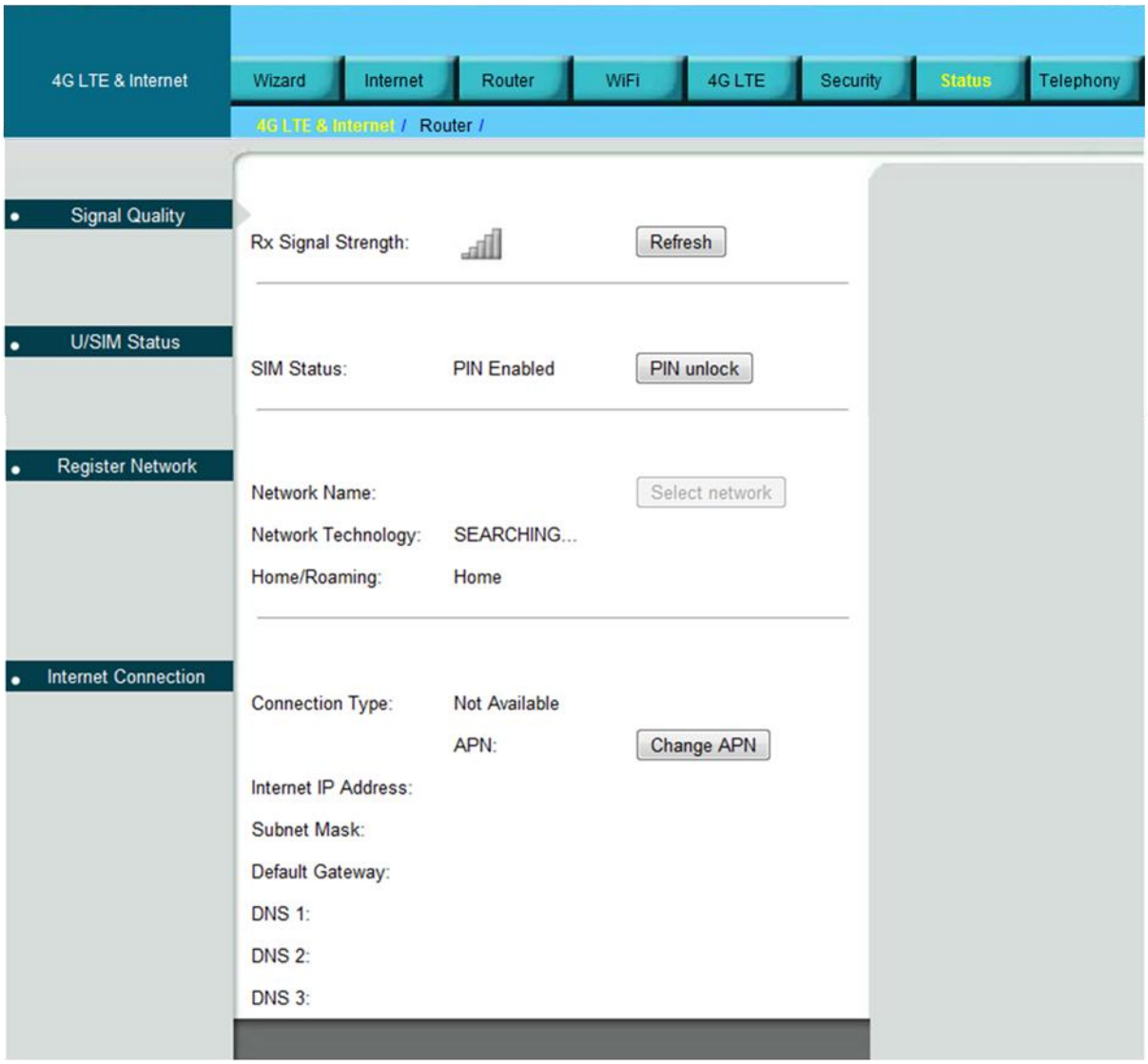
1. Enter a name for your voice device.
2. Enter the MAC address of your voice device.
3. Select the appropriate priority: **High**, **Medium**, **Normal**, or **Low**.
4. Click **Add** and **Save Settings** to save your changes.

Summary

This lists the QoS entries you have created for your applications and devices. Select **Edit** to edit an item or **Remove** to remove the item. Preset items cannot be edited.

Status

4G LTE & Internet



Signal Quality

When you access the Internet via a mobile network, click **Refresh** to show the signal strength.

U/SIM Status

Your SIM card verification status is shown in this area. Clicking **Pin unlock** displays the **PIN Verification** tab.

Register Network

Network Name: This shows the name of your network operator.

Network Technology: This shows the network technology you are currently using.

Home/Roaming: This indicates whether the Router is in Home or Roaming status.

Clicking **Select network** displays the **Preferred Network** tab.

Internet Connection

Connection Type: This indicates the type of Internet connection you are using.

Internet IP Address: This is the Router's IP Address, as seen on your local network.

Default Gateway: The Router’s Default Gateway address is displayed here for DHCP and static IP connections.

Clicking **Change APN** displays the **Internet > Basic Setting** tab.

Router

Firmware Information

Firmware Version: This is the Router's current firmware.

Modem Version: This is the LTE/3G Module's current firmware.

Current Time: This shows the time, as you set on the Optional tab.

Local Network

Local MAC Address: This is the Router's MAC Address, as seen by your ISP

Router IP Address: The Router's IP Address that appears on your local network.

Subnet Mask: This shows the current subnet mask being configured for your local network.

DHCP Server: The status of the DHCP server function is displayed here. Clicking the **Change** button displays the **Network Setting** tab.

Start IP Address: This shows the beginning of the range of IP Addresses used by devices on your local Ethernet network.

End IP Address: The end of the range of IP Addresses used by devices on your local Ethernet network is shown here.

DHCP Client Table: Click this button to open a screen showing you which PCs are utilizing the Router as a DHCP server.

WiFi Network

MAC Address: This is the Router's MAC Address, as seen on your local wireless network.

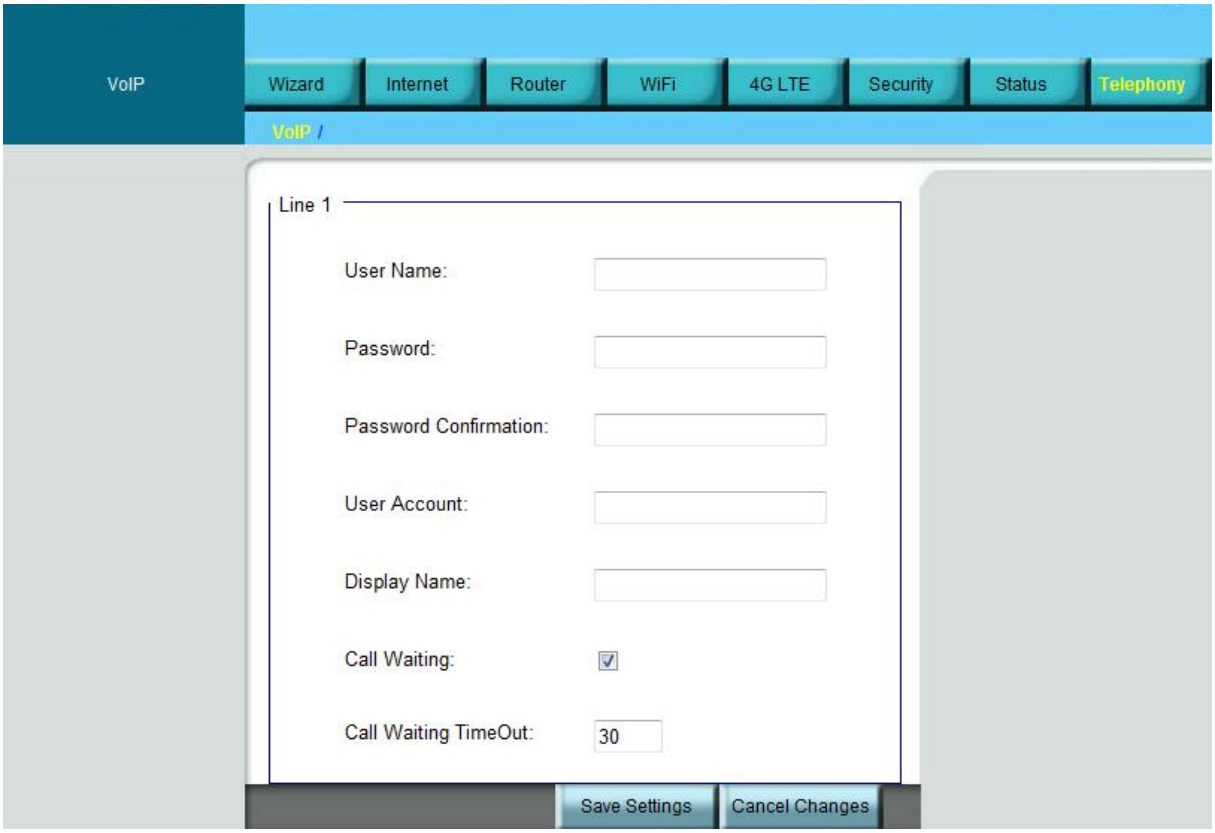
Mode: This displays the wireless mode (802.11b/g/n, 802.11b/g, 802.11b, 802.11g, 802.11n) used by the network.

Network Name (SSID): This displays the wireless network name or SSID. Clicking **Change** button displays the **Basic WiFi Network** tab.

Standard Channel: This displays the channel on which your wireless network is broadcasting.

Telephony

VOIP



VOIP

VOIP allows the user to connect a standard analog phone to the router via the RJ-11 jack and make voice calls over the internet. Use the information provided by your ISP or VOIP service provider to complete the relevant fields.

Appendix A: FAQ

Q: What does the Power LED indicate?
A: The Power LED with solid yellow indicates the Router is on.

Q: How to connect to the Router?
A: 1. Connect an Ethernet cable between the PC/NB and the Router.
2. Use WiFi to connect.

Q: What's the default "User name" and "Password" for the Router?
A: Please refer to the Quick Start Guide included in the package.

Q: How to enter GUI?
A: 1. Connect PC/NB to the Router.
2. Open Internet Explorer or another Web browser.
3. Input "http://192.168.1.1" (default) or "http://R500.ROUTER".
4. Input User name and Password.
5. Please refer to the Quick Start Guide included in the package.

Q: How to setup the configuration for the Router?
A: 1. Enter Wizard page to setup.
2. Enter each GUI page to setup.

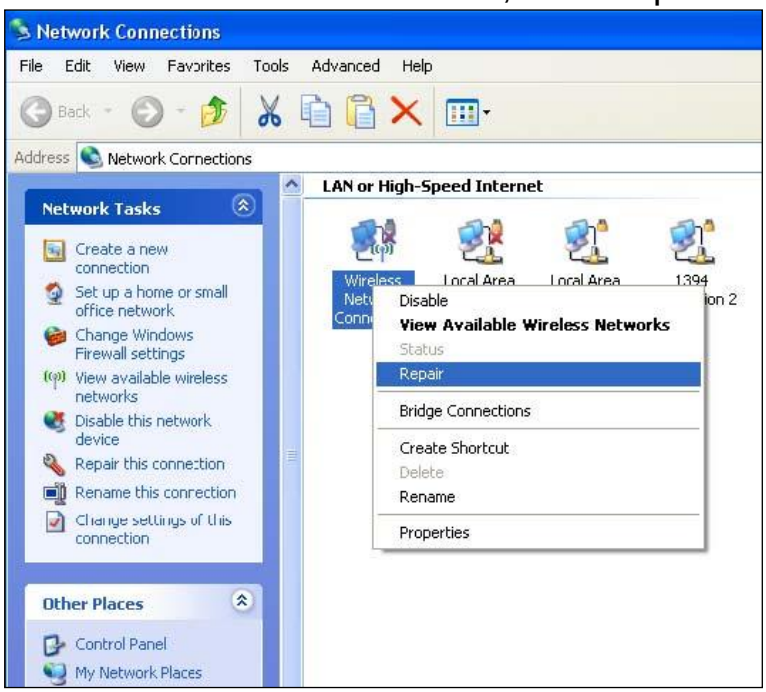
Q: Why can't I connect to the network via built-in LTE/3G module?
A: 1. Check if the SIM/USIM is inserted well.
2. Check if the type of radio access technology on the screen if the network is available.
3. Check the subscriber's network operator on the screen if the ISP name is available.
4. Check if the Status on GUI if the SIM/USIM is detected well.
5. Check if the Status on GUI if the APN it is correct.

Q: Why can't I link on the GUI?

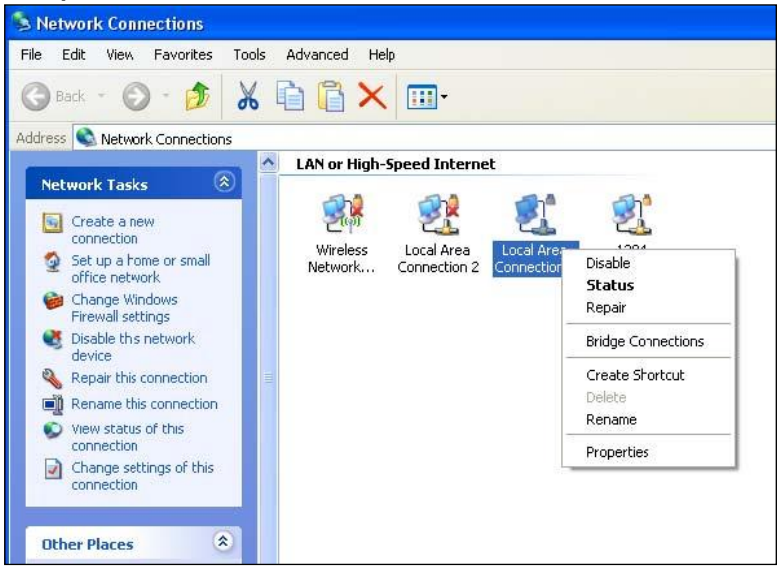
A: If you have changed your WiFi security, SSID, Local IP address, you have to repair your network to get a new IP so that you can link the GUI.

XP:

If you are a WiFi user, click Network Connections and right click on Wireless Network Connection, click Repair.

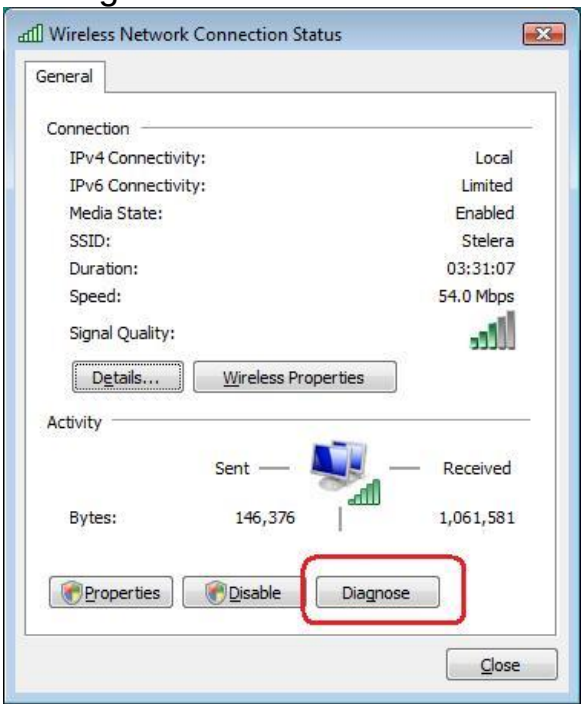


If you use Local Area Connection to connect the Router, click Network Connections and right click on Local Area Connection, click Repair.

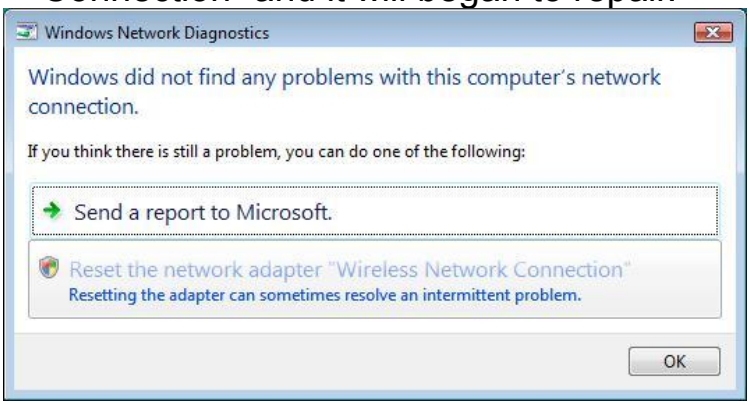


Vista/Win 7:

1. If you are a WiFi user, please click Network and Sharing Center > Manage network connections > Wireless Network Connection > Diagnose



2. Please click Reset the network adapter “Wireless Network Connection” and it will began to repair.


Windows Network Diagnostics
Windows did not find any problems with this computer's network connection.
If you think there is still a problem, you can do one of the following:
Send a report to Microsoft.
Reset the network adapter "Wireless Network Connection"
Resetting the adapter can sometimes resolve an intermittent problem.
OK

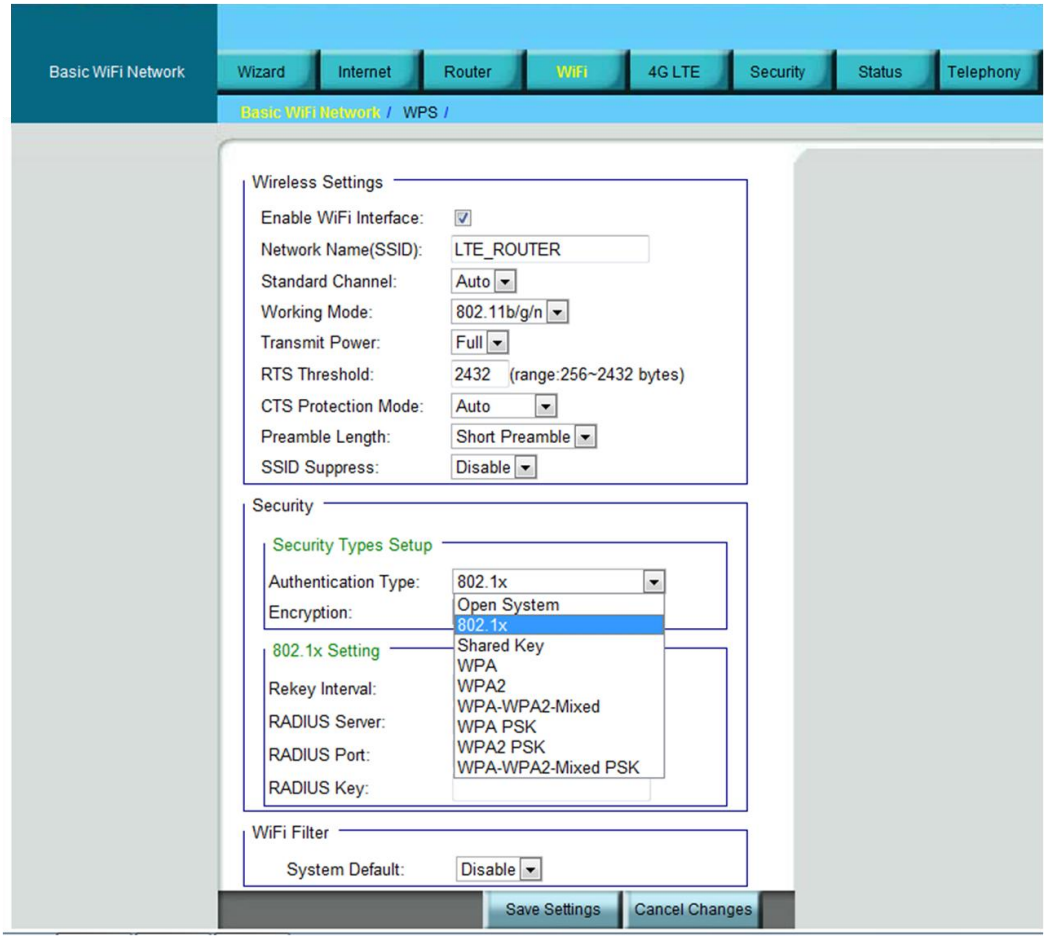
3. If you use Local Area Connection to connect the Router, please click Network and Sharing Center > Manage network connections > Local Area Connection > Diagnose, do the step 1 and following the message to repair it.

Q: How to setup my WiFi settings from GUI?

A: Entering the GUI first then click WiFi > Basic WiFi Network, you can setup your basic WiFi settings here.

If you want to set your WiFi Security please click “Basic WiFi Network”.

There are nine wireless security mode options supported by the Router: Open System, 802.1x, Shared Key, WPA, WPA2, WPA-WPA2-Mixed, WPA PSK, WPA2 PSK, WPA-WPA2-Mixed PSK.

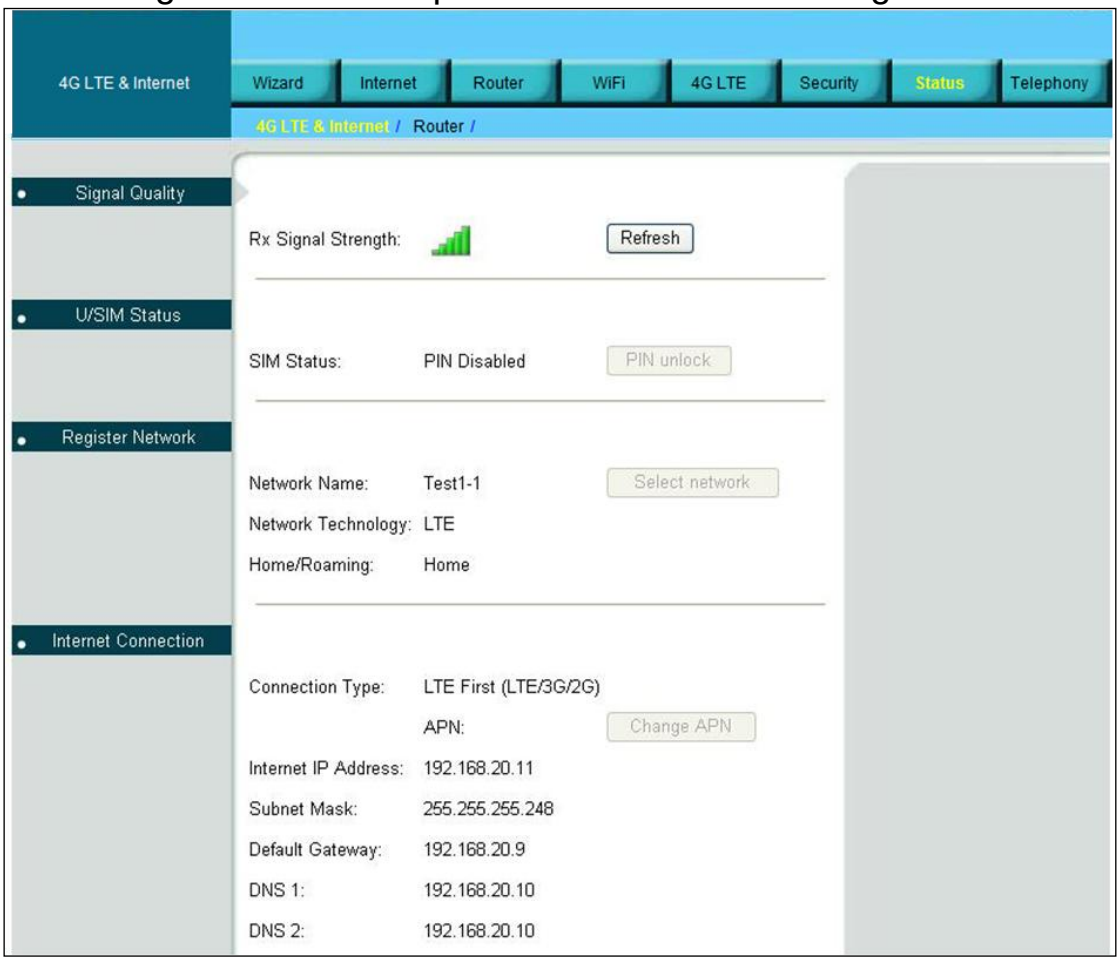


Q: What should be noted when 802.11n is selected?
A: For higher data transfer throughput, ensure that the router is not configured to use WEP or TKIP

A: Is there any limitation for the WPS function?
Q: If you want to use WPS function, make sure that the router is not configured to use WEP as its encryption in Basic WiFi Netwok > Security Type Setup.

Q: Why can't I use the Router in the office?
A: Your Router's IP address might be in conflict with the office default settings.

Q: Why is my internet speed so slow with Router?
A: 1. You can check the GUI Status > Signal Quality, the Rx Signal Strength. If the footstep is too low it means the signal is too weak.



2. You can go to the GUI WiFi > Basic WiFi Network, change the Standard Channel to others then save.

Q: Why can't I use VPN via Router?

A: You may check your office IP settings, the IP settings must not conflict with each other.

Q: How do I do the settings when I use xDSL to link the Router?

A: 1. PPPoE: Go to the GUI Internet > Basic Setting, select Ethernet as Connection Type,> Ethernet Setting. Change Connection Type to PPPoE, and fill in the Username and Password which provided by your ISP. Remember to connect your xDSL or Modem to the WAN Port on your Router.

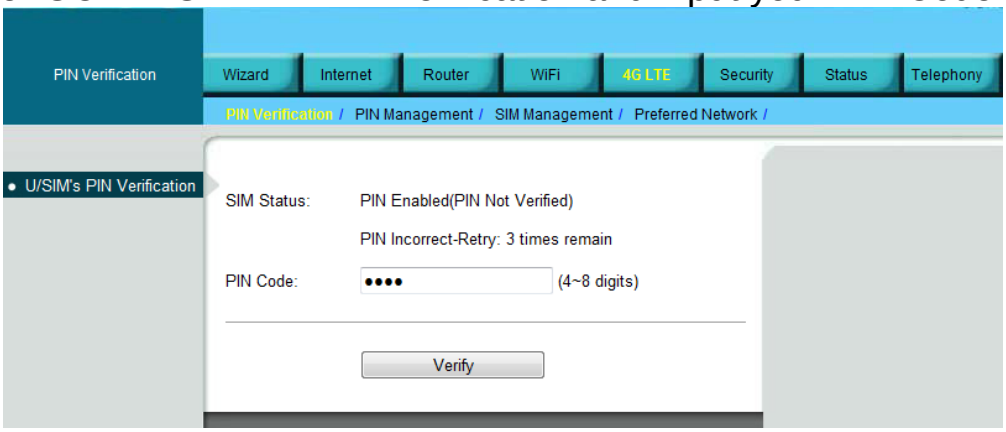
Q: Can I prevent others from using my Router?

A: Yes, there are some ways to prevent others from using your Router.

1. Enable your WiFi client filter.
2. Disabled your SSID Suppress.
3. Setting your WiFi security.

Q: My PIN code is enabled and where can I input the PIN code to use my Router?

A: Enter GUI > 4G LTE > PIN Verification and input your PIN Code.



Q: Why does my SIM status display "Read SIM Fail", what can I do?

A: You can check the SIM card is inserted correctly in your router.

Q: How to use the Reset button on the Router?

A: 1. Short press of the Reset can restart the Router.

2. Long press of the Reset for more than 5 sec can reset the Router to factory default.

Q: Where can I reset the Router to factory default?

A: 1. Long press of the Reset button on the Router for more than 5 sec.

Appendix B: Specification

Note: Specifications are subject to change without notice.

Physical	
Wi-Fi	802.11 b/g/n (2x2 MIMO)
Modem	Embedded, LTE/EVDO
Modem Chipset	Qualcomm MDM9200 + RTR8600
Dimension (LxWxH, mm)	99 x 127.5 x 24.1 mm
Weight (g)	170g
Interface	
Power On/Off Switch	Yes
WPS Button	Yes
LAN port	RJ45 x 1
WAN port	RJ45 x 1
Telephone port	RJ11 x 1, POTS port for standard analog phone connection
Power supply plug	Yes
Reset button	Long push (>5s): Reset to factory default setting Short push: device reset
SIM slot	Yes
LCD Display	Yes
Connectivity and Data Speed	
LTE Band	Band 2/4/12/17/25
LTE Bandwidth	5 MHz /10 MHz /15 MHz /20 MHz
LTE Data Rate	Downlink: up to 100Mbps, Uplink: up to 50Mbps
EVDO Band	AWS/800/PCS 1900MHz
WLAN	802.11b/g/n
Voice call	VOIP
Antenna	
Cellular Main Antenna	Embedded
Cellular Rx Diversity Antenna	Embedded, diversity band at Band 2/4/12/17/25
Cellular External	Yes x 2

Antenna port	
Wi-Fi Antenna	Embedded
Wi-Fi External Antenna	Yes x 1
Router Features	
Security	Multiple VPN pass-through (IPSec, PPTP, L2TP), Internet access restriction, Firewall, DoS Prevention, Traffic and Event Logging
NAT-NAPT	Port forwarding, Port triggering, DMZ, Multicast Pass-Through, Static Routing, Dynamic Routing (RIP1, RIP2), QoS
DNS	DNS Agent, DDNS
ALG Support	Yahoo messenger, AOL messenger, MSN messenger, ICQ, RealAudio, NetMeeting, Telnet, FTP, Microsoft Traceroute, Quake, IRC, Microsoft PPTP Client
Other features	IPv4, TCP, UDP, ICMPv4, ARP, DHCP Server/Client, HTTPs, NTP, TFTP server, MAC Clone, RTP, RTCP, DiffServ, TOS, SNTP
Browser-based Administration GUI	Setup Wizard in GUI. Browser supported: IE, Firefox, Safari, Chrome
Browser-based Administration GUI Multi-Language Support	English
VOIP Function	
Voice Telephony	RJ-11 for analog phone, VoIP codec
Voice Signaling	SIP(RFC3261, 3262, 3264)
Wireless LAN	
802.11b data rate	1/2/5.5/11 Mbps, Auto or Fixed Rate
802.11g data rate	1/2/5.5/11/6/9/12/18/24/36/48/54 Mbps, Auto or Fixed Rate
802.11n data rate	65/135/270(2x2 MIMO) Mbps, Auto or Fixed Rate
Security	WPA2/WPA/AES/TKIP, WPA/WPA2 PSK mode, 802.1x (identify all EAP types supported), None/64/128 bits WEP Encryption, MAC filter, open system and shared key authentication, SSID Broadcast Disable, WPS.
Other Functions	

Automatic APN / ID / password settings	Yes
APN updateThrough browser-based GUI	Yes
Support FW version upgrade	Yes.
System protection	Password protected system reset to factory default, Password protected administrator and user access authority (provisioning, configuration, authentication).
Status Indication	
LCD Display	[Status Bar] • Cellular Signal Strength • Radio Technology • Wi-Fi, Ethernet, SIP status • Roaming indication • SMS Notification [Main Screen] • Network Operator Name • Greetings • WPS Active Mode with count down timer • Time and Date
Accessories	
Power adaptor	Supported, Input - 100~240V 50~60Hz AC, output – 12V/12A
Environment	
Operation Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-20°C to 60°C (-4°F to 140°F)
Operating Humidity	10% to 80% Non-Condensing
Storage Humidity	5% to 90% Non-Condensing
Certification	
	FCC, GCF conformance
	RoHS

Appendix C: Important Safety Information and Glossary

Europe – EU Declaration of Conformity

CE

European Union Notice
Products with CE marking comply with the R&TTE Directive (99/5/EC), the EMC Directive (2004/108/EC), and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community.
Compliance with these directives implies conformity to the following European Norms (in parentheses are the equivalent international standards).

EN 60950-1 (IEC 60950-1)
Safety of Information Technology Equipment.

EN 300 328
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; data transmission equipment operating in the 2.4 GHz ISM band and using spread spectrum modulation techniques.

EN 301 489-24
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 24: Specific conditions for IMT-2000 CDMA direct spread (UTRA) for mobile and portable (UE) radio and ancillary equipment.

ETSI EN 301 511
Global system for mobile communications (GSM); Harmonised EN for mobile stations in the GSM 900 and GSM 1800 bands, covering essential requirements of article 3.2 of the R&TTE directive (1995/5/EC).

ETSI EN 301 489-1
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements.

ETSI EN 301 489-7
Electromagnetic compatibility and Radio spectrum Matters (ERM); Electromagnetic Compatibility (EMC) standard for radio equipment and services; Part 7: Specific conditions for mobile and portable radio and ancillary equipment of digital cellular radio telecommunications systems (GSM and DCS).

ETSI EN 301 489-17
Electromagnetic compatibility and Radio spectrum Matters (ERM);
Electromagnetic Compatibility (EMC) standard for radio equipment and services;
Part 17: Specific conditions for 2.4 GHz wideband transmission systems.

ETSI EN 301 908-1 & -2
Electromagnetic compatibility and Radio spectrum Matters (ERM); Base Stations (BS), Repeaters and User Equipment (UE) for IMT-2000 Third Generation cellular networks;
Part 1: Harmonised EN for IMT-2000, introduction and common requirements, covering essential requirements of article 3.2 of the R&TTE Directive.

EN 50385
Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz - 40 GHz) - General public.

Federal Communication Commission Interference Statement

15.21
You are cautioned that changes or modifications not expressly approved by the part responsible for compliance could void the user's authority to operate the equipment.

15.105(b)

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference and
2) This device must accept any interference received, including interference that may cause undesired operation of the device.

FCC RF Radiation Exposure Statement:
1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

Glossary

APN (Access Point Name/Network): Provides routing information. Consists of:

Network ID: Identifies the external service requested by an user.

Mobile network operator ID: Specifies routing information.

ARFCN (Absolute Radio Frequency Channel Number): The specific ID numbers for all radio channels used in cellular mobile communications.

bps (bits per second): How data flow is measured.

CHAP (Challenge Handshake Authentication Protocol): CHAP identifiers are changed frequently and authentication can be requested by the server at any time.

DNS (Domain Name System): Helps route network traffic by making the addressing process more user-friendly.

DHCP (Dynamic Host Configuration Protocol): How devices obtain IP addresses from a server.

DUN (Dial-Up Network): Windows component that enables online access via a modem.

IMEI (International Mobile Equipment Identity): A number unique to each GSM/UMTS device that can be used block network access by a stolen mobile device.

IP (Internet Protocol): Routes packets over a network.

Kbps (Kilobits per second): A data flow measure; 1024 bits/second.

LAN (Local Area Network): A data network with limited range but good bandwidth.

LTE (Long Term Evolution): Fourth generation cellular technology featuring data speeds of up to 100Mbps downlink and 50Mbps uplink. Additional features include MIMO transmissions and an all IP based network.

Mbps (Megabits per second): A data flow measure; 1,048,576 bits/second.

PAP (Password Authentication Protocol): The difference between PAP authentication and a manual or scripted login, is that PAP is not interactive. The username and password are entered in the client's dialing software and sent as one data package as soon as the modems have established a connection, rather than the server sending a login prompt and waiting for a response.

PPP (Point-to-Point Protocol): An internet connection method.

PIN (Personal Identity Number): Four to eight digital numbers SIM card security code; allows access to the carrier’s network.

Rx: Shorthand for Reception.

SIM (Subscriber Identity Module): A small card that contains key mobile device identification, subscription and contact information.

Tx: Shorthand for Transmission.